International Labour Organization

ILO Working Paper 149

September / 2025

Navigating workers' data rights in the digital age

A historical, current, and future perspective on workers' data protection

Author / Halefom Abraha

ISBN 9789220426319 (print), ISBN 9789220426326 (web PDF), ISBN 9789220426333 (epub), ISBN 9789220426340 (html). ISSN 2708-3438 (print), ISSN 2708-3446 (digital)

https://doi.org/10.54394/MLUH5441

Suggested citation:
Abraha, H. 2025. *Navigating workers' data rights in the digital age: A historical, current, and future perspective on workers' data protection*, ILO Working Paper 149 (Geneva, ILO). https://doi.org/10.54394/MLUH5441

Abstract

Over recent decades, comprehensive data protection legislation has proliferated worldwide, with a majority of jurisdictions enacting robust statutory regimes. Despite this abundance of legal standards, persistent challenges remain regarding the efficacy of these laws in protecting individuals–particularly workers–within the increasingly digitalised workplace. Workers are especially susceptible to harm due to entrenched power asymmetries and heightened risks of data exploitation, yet many existing legal frameworks provide insufficient or inconsistent protection, and some jurisdictions explicitly exclude workers from coverage.

This research critically examines the multidimensional risks associated with workplace digitalisation and systematically analyses regulatory challenges and protection gaps across diverse jurisdictions. By integrating historical analysis, current policy initiatives, and comparative cross-jurisdictional perspectives, the study identifies structural deficiencies in prevailing approaches. It concludes by proposing policy solutions to advance worker-centric data governance frameworks, tailored to address the distinctive challenges of contemporary labour relations and to ensure more equitable and effective protection for workers in the digital age.

About the authors

Dr. Halefom Abraha is an Assistant Professor of law and technology at Utrecht University School of Law and a member of the Netherlands Institute of Human Rights (SIM). His research and teaching interests focus on workers' data rights and the regulation of AI and algorithmic management in the labour market. He also researches cross-border data access in the context of law enforcement and digital sovereignty.

Table of contents

▶ Introduction

Aim and Scope

The emergence of data protection laws in the late 1970s marked the initial regulatory response to societal risks posed by the information revolution, particularly those associated with automated data processing. While more than 162 countries now have comprehensive data protection laws, a recurring challenge lies in their applicability to the world of work and their adequacy in protecting individuals in an increasingly digitalised workplace.

Thirty-five years ago, Spiros Simitis questioned whether omnibus data protection frameworks could address the unique complexities of workplace dynamics, advocating instead for employment-specific rules. His critique resonates urgently today, as pervasive digital surveillance and algorithmic management systems amplify workplace power dynamics, posing novel risks to workers' fundamental rights that existing regulations have failed to adequately address.

Workers — particularly vulnerable due to systemic power asymmetries and data exploitation risks — often receive inadequate protection under existing laws, with some jurisdictions excluding them entirely. Historically, policymakers have acknowledged this inadequacy, as evidenced by the Council of Europe's 1989 Recommendation on the protection of workers' personal data, the ILO's 1997 Code of Practice on Protection of Workers' Personal Data, and the European Union's 2001 Opinion on employment data processing, each adopting workplace-specific rules to complement general regulations. Yet translating this recognition into robust legislative frameworks at national levels has proven largely unsuccessful, reflecting entrenched regulatory gaps.

Furthermore, the technological landscape has undergone significant transformation since the publication of these international instruments. All frameworks are non-binding, and they were adopted before the widespread implementation of electronic monitoring systems in workplaces and the dawn of the AI era. The emergence of data-driven people management and automated decision-making has introduced new challenges that these earlier frameworks were not designed to fully address.

It is therefore unsurprising that the ILO has refocused its attention on this issue. In March 2024, the ILO Governing Body decided to convene at a future date a tripartite meeting of experts on the protection of workers' personal data in the digital era. This development underscores the recognized need for updated and comprehensive standards for workers' data protection that establish a fair balance between workers' fundamental rights and employers' interests.

Against this background, this research examines the multidimensional risks of workplace digitalisation and analyses regulatory challenges and gaps across jurisdictions. By synthesising historical precedents, current initiatives, and cross-jurisdictional comparisons, it proposes policy solutions to advance worker-centric data governance frameworks capable of addressing modern labour relations' unique challenges. Ultimately, the research aims to contribute to the development of more robust, human-centred data protection frameworks and standards that are adaptable to the evolving landscape of work in the digital age, while also promoting innovation and protecting business interests.

The research is subject to limitations regarding geographic and material scope. In addition to international standards, the study systematically analyses regulatory frameworks of selected

jurisdictions, with particular focus on the European Union, the United States, and Australia – regions characterised by multiple regulatory initiatives and distinctive approaches. The research also examines frameworks and recent developments in India, China, Brazil, and several African countries. While the selection aims to be representative of major jurisdictions, it does not mean to suggest that the research provides comprehensive coverage of all global regions. Substantively, the research addresses existing regulatory frameworks, including data protection and privacy laws, labour laws, algorithmic management and AI regulations, non-legislative guidelines, and recent policy initiatives. Although the research seeks to highlight key regulatory frameworks within each jurisdiction, it does not claim to be exhaustive. Nuanced local interpretations and sector-specific regulations may fall outside the scope of this analysis.

Use of Terms

Unless otherwise explicitly indicated, this research uses the term 'worker' to include any current or former worker or applicant for employment and independent contractors. The objective is to ensure that that workplace data protection rules provide consistent protections at all stages of the employment relationship, regardless of its legal nature or status. This approach is further explained in Section 6.2. in some instances, the term 'employee' may be used when it appears in specific regulations or is directly quoted from other sources.

Structure

The research is organized in six parts. The next section examines the prevalence of advanced workplace technologies, focusing on digital monitoring and automated decision-making systems. Section 3 analyses the risks these technologies and practices pose to workers' data rights, including privacy as well as broader social and labour rights. Section 4 maps existing legal protections at the international level and across selected jurisdictions. Section 5 identifies the gaps, challenges, and uncertainties within these regulatory frameworks. Finally, Section 6 proposes potential pathways for future regulations to effectively address these issues effectively.

1 Workplace monitoring and decision-making technologies

In the past few decades, data-driven technologies have transformed the world around us, particularly the workplace. While the precise scope and nature of how recent technological advancements, such as AI, will change the world of work remain uncertain, employers are increasingly using data and algorithms in ways that may potentially have consequences for workers' fundamental rights and interests.

The digitalisation of the workplace has recently garnered considerable media attention and public debate around the world. Specifically, the rapid advancement and widespread adoption of powerful algorithmic systems and surveillance tools in the world of work have prompted many commentators to re-examine and question whether existing regulatory systems are adequately equipped for the digital era.[1] This technological transformation presents both opportunities and risks that need careful consideration and balanced regulation.

Collecting and processing workers' data is an inherent prerogative of the employer, an essential consequence of the employment relationship. Employers collect a range of workers' personal data for many justified and often necessary reasons, or as required by law. While employers use a wide range of tools to gather and process workers' data, and these practices take many forms, this research focuses on two broad categories of workplace technologies and practices: *digital monitoring/surveillance* [2] *and algorithmic management*. This focus does not suggest that more traditional methods of data processing do not pose privacy and data protection risks. Rather, it is to encourage policymakers to pay more attention to employers' new acts or practices and methods of processing instead of fixating on the data itself.

Automated monitoring and surveillance systems can be defined as technologies used for, or in support of, monitoring, supervising or evaluating work performance, worker behaviour, or the activities carried out within the work environment and beyond. These systems can range from simple time-tracking software to sophisticated biometric surveillance tools. On the other hand, algorithmic management or automated decision-making systems encompass algorithmic tools used to support, augment, or fully replace managerial decisions that affect working conditions.[3] These systems can influence various aspects of employment, including access to work, earnings, occupational safety and health, working time, promotion and contractual status, and disciplinary as well as termination procedures.

It is important to note that this classification is not meant to suggest that these technologies and practices are mutually exclusive. In fact, they often reinforce and complement each other, creating complex ecosystems of digital workplace management. For instance, data collected through automated monitoring systems are often feed into algorithmic management systems, influencing decisions about worker performance, scheduling, or promotions. As Fernandez Macias and others

1 Jeremias Adams-Prassl and others, 'Regulating Algorithmic Management: A Blueprint' (2023) 14 European Labour Law Journal 124.

2 The terms 'monitoring' and 'surveillance' are used interchangeably for the purpose of this research. However, it's important to note that employee surveillance is generally perceived as more intrusive and ethically problematic than employee monitoring, as it extends beyond work-related activities. see Eurofound, *Employee Monitoring and Surveillance: The Challenges of Digitalisation* (Publications Office of the European Union, Luxembourg 2020).

3 Adams-Prassl and others (n 4).

pointed out, algorithmic management of work generally presupposes some degree of digital monitoring, which provides the data on which the algorithms operate.[4] For this research, these systems are treated separately only to the extent that they raise unique legal and policy issues.

Digital monitoring and surveillance at work

Workplace monitoring and surveillance is not a new phenomenon,[5] nor is the utilization of modern technologies to do so. The capabilities and implications of workplace technologies and the need for workers' data protection legislation have been debated since the 1970s.[6] However, recent advances in workplace monitoring and surveillance technologies, coupled with the increasing digitalization of the workplace have, according to the Eurofound, 'made them more pervasive and ubiquitous and potentially more intrusive, pushing the boundaries of acceptability and posing new challenges for legislators and policymakers'.[7]

Employers are increasingly utilizing sophisticated electronic monitoring and surveillance tools to track their workers' every move and predict a wide range of worker behaviours in the workplace. These systems 'enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles and wearables'.[8] While some uses may be positive − such as signalling to management if a worker enters a hazardous zone in a construction site − other uses may be less so, such as when data collected on 'whom [workers] talk to, what they type, how quickly they complete tasks and even their mood'.[9] Indeed, the extent of worker monitoring is no longer limited to performance management; workers' thoughts, feelings and physiology can equally be tracked and analysed, and their behaviour predicted.[10] Big data and people analytics[11] tools allow for new types of systematic and data processing at work, enabling employers to obtain an increasingly detailed and sophisticated picture of what workers are doing and how they feel about their work.[12]

Comparing to traditional forms of monitoring, Ravid et al (2020) succinctly summarised the impact of new workplace monitoring and surveillance technologies and practices as follows:

> *Employers (...) can track individual employees continuously, randomly, or intermittently; discreetly or intrusively; and with or without warning or consent (...). As a result, (new monitoring and surveillance technologies) capture behaviour in great detail, generating rich, permanent records that managers can quickly access and that may or may not relate directly to performance (...). (They) can also target internal states and private behaviors. For example, e-mail monitoring allows organizations to track employee thoughts,*

4 European Commission Joint Research Centre, *The Platformisation of Work: Evidence from the JRC Algorithmic Management and Platform Work Survey (AMPWork).* (Publications Office of the European Union 2023) <https://data.europa.eu/doi/10.2760/801282> accessed 16 November 2024.

5 Frederick Winslow Taylor, *The Principles of Scientific Management* (Dover Publications 1997); Marx Gary T. and Sanford Sherizen, 'Monitoring on the Job: How to Protect Privacy as Well as Property' (*Technology Review*, 1986) <https://web.mit.edu/gtmarx/www/privacy.html> accessed 16 November 2024 (noting that contemporary monitoring is a continuation of Taylorism, though new developments in electronic technology are taking that ethos to new heights).

6 For detailed analysis on long history of work monitoring and its implications, see 'Personal Privacy in an Information Society' (US Privacy Protection Study Commission 1977); 'The Electronic Supervisor: New Technology, New Tensions' (US Congress, Office of Technology Assessment, September 1987).

7 Sara Riso, 'Monitoring and Surveillance of Workers in the Digital Age' (Eurofound) <https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age> accessed 16 November 2024.

8 Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017.

9 Charlotte Garden, 'Labor Organizing in the Age of Surveillance' (2018) 63 St. Louis U. L.J.

10 Kirstie Ball, 'Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations' (Publications Office of the European Union, JRC125716 2021).

11 Matthew T Bodie and others, 'He Law and Policy of People Analytics' 88 U. COLO. L. REV.

12 Garden (n 12).

> *feelings, and attitudes that are expressed in electronic exchanges but not outwardly. Social media monitoring allows organizations to track the social networks and relationships that employees build inside and outside of the workplace. Recent (monitoring and surveillance) technologies allow for the tracking of employees' physiological states, providing organizations with biometric information, such as heart rates and body heat emissions (...).*[13]

A number of technologies can be used for worker monitoring and surveillance for a host of different purposes, targeting different aspects of working life. In this regard, the most common monitoring and surveillance practices can be categorized as *performance* monitoring, *behaviour* monitoring, *personal characteristics* monitoring.[14]

Behaviour monitoring and *performance tracking* technologies have become ubiquitous in the workplace across sectors, particularly in low-paying jobs. These technologies range from the more conventional form of monitoring such as CCTV surveillance and monitoring of emails, telephone calls and internet usage to more sophisticated biometric technologies, predictive analytics and AI. For instance, GPS and radio-frequency identification (RFID) devices are often used to provide always-on and real-time location tracking of the whereabouts of workers. According to a 2022 New York Times article, eight out of 10 of the largest private employers in the US track the productivity metrics of individual workers, many in real time.[15]

Employment monitoring systems can track workers' computer activities, including mouse movement and the number of keystrokes, take screenshots etc. Many workers are subject to trackers, scores, 'idle' buttons, or just quiet, constantly accumulating records. Pause can lead to penalties, from lost pay to lost job,[16] 'potentially requiring employees to justify every break or interruption'.[17] For instance, if workers have to get up from their desk to take a break, go to the bathroom, or get lunch, their mouse is no longer active, and their status will turn from active to idle. In some instances, such as freelancing platforms[18] and some logistics companies,[19] the workers are only paid for those minutes when the system detected active work.

Wearable technologies, such as smartwatches, smart bracelets and smart glasses with built-in GPS capabilities and sensors tracking movements and location and counting steps and pulses, are emerging trends in the workplace. Some employers use FitBit bracelets to track workers' fitness, sleep quality, fatigue levels and location.[20] Warehouses workers in various jurisdictions are required to use hand-held scanners (wearable devices) which monitor every movement of every worker, including toilet breaks.[21] The German's Lower Saxony State Data Protection Commissioner

---

13 Daniel M Ravid and others, 'EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring' (2020) 46 Journal of Management 100.

14 'The Electronic Supervisor: New Technology, New Tensions' (n 9); Eurofound (n 5); 'Workers' Privacy Part II: Monitoring and Surveillance in the Workplace' (International Labour Office, Conditions of work digest, Vol 12 Number 1, 1993); Ball (n 13).

15 Jodi Kantor and others, 'The Rise of the Worker Productivity Score' *The New York Times* (15 August 2022) <https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html> accessed 11 November 2024.

16 Lauren Kaori Gurley, 'Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts' (*VICE*, 2 June 2022) <https://www.vice.com/en/article/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts/> accessed 11 November 2024; Kantor and others (n 18).

17 'Employee Monitoring: CNIL Fined AMAZON FRANCE LOGISTIQUE €32 Million' <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> accessed 18 November 2024.

18 Kantor and others (n 18).

19 'NLRB Memo Takes Aim at Intrusive Workplace Surveillance & Algorithmic Management Systems' (*Center for Democracy and Technology*, 21 December 2022) <https://cdt.org/insights/nlrb-memo-takes-aim-at-intrusive-workplace-surveillance-algorithmic-management-systems/> accessed 1 May 2025.

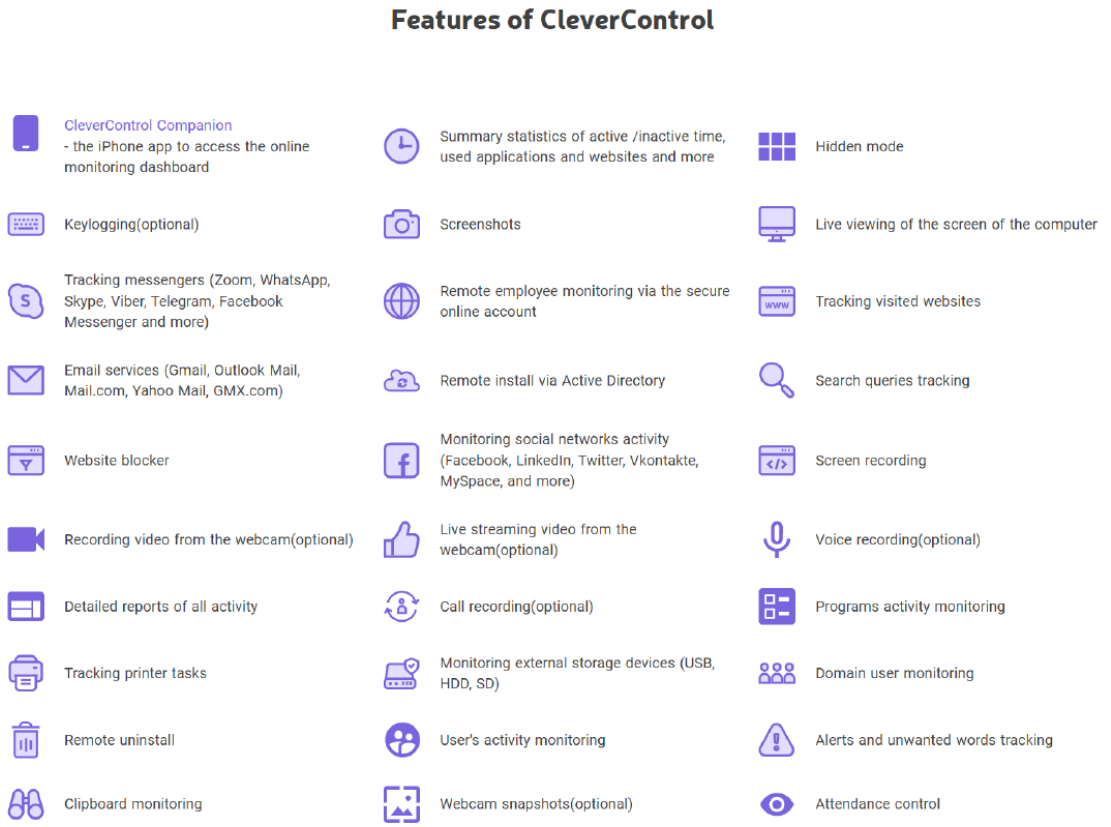
20 David Cox, 'The Rise of Employee Health Tracking' (*BBC*, 11 November 2020) <https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking> accessed 26 November 2024.

21 Jay Stanley, 'Amazon Drivers Placed Under Robot Surveillance Microscope' (*American Civil Liberties Union*, 23 March 2021) <https://www.aclu.org/news/privacy-technology/amazon-drivers-placed-under-robot-surveillance-microscope> accessed 12 November 2024.

characterised this practice as 'total surveillance' of the workers, which could constitute a serious interference with the right to privacy without justification.[22]

The extent and pervasiveness of performance and behaviour monitoring and tracking technologies can be illustrated by the figure below. Some of the most invasive worker monitoring tools can be deployed remotely and secretly monitor workers' every move and activity across devices, including secretly activating webcams (to track eye movements, body language, and facial expression to assess attentiveness and infer stress) and microphones.[23]

▶ **Figure 1: A screenshot from the employee monitoring tool 'CleverControl'**



More advanced technologies such as biometrics, emotion recognition and predictive people analytics tools and data-mining techniques are also increasingly creeping into the workplace to monitor workers' *personal characteristics* and to make predictions about workers' behaviour.[24] Biometric technologies, which encompass processes used to recognize, authenticate, and identify individuals based on physical and/or behavioural characteristics, have become increasingly prevalent in modern workplaces.[25] These technologies, ranging from fingerprint and facial recognition to iris scans, are primarily employed for access control to buildings, rooms, systems, and devices across sectors including construction, healthcare, rental, and transportations. Beyond security applications, biometrics are also integrated into time and attendance systems, replacing traditional

22 *Regional Administrative Court of Hannover, Case 10 A 6199/20 February 8, 2023*.
23 See 'Employee Monitoring Software' (*iMonitorSoft*) <https://www.imonitorsoft.com/> accessed 25 July 2023.
24 Eurofound (n 5).
25 'Bossware: The Dangers of High-Tech Worker Surveillance & How to Stop Them' (Big Brother Watch, September 19 2024).

methods like swipe cards and PIN numbers. The adoption of biometric timekeeping has streamlined workplace management, enhancing accuracy and reducing time fraud. Moreover, biometrics have found their way into 'corporate wellness' programs, where workers are encouraged to self-track using body-worn devices.[26] This expansion of biometric uses in the workplace, while offering efficiency and security benefits, raises significant privacy and ethical risks, as discussed below.

Furthermore, predictive analytics tools and data-mining technologies are sometimes used to predict workers' future behaviour and assign 'risk scores', including predicting likelihood of quitting.[27] Emotion recognition techniques have been used to detect job applicants' emotional expressions, matching them with personality traits with the intent of screening out prospective applicants with 'undesirable' characteristics.[28] Some of these products claim to track emotions such as anger, contempt, disgust, engagement, joy, sadness, and surprise by analysing a video clip.

Even seemingly benign techniques such standardized questions have been used with the intent of detecting workers' mood or behaviour. For instance, some companies are implementing software systems designed to monitor workers' sentiment and behaviour. These systems often feature regular pop-up surveys that prompt workers to 'voluntarily' respond to standardized questions about their emotional state throughout the workday. Response options typically include 'frustrated', 'stressed', or 'motivated'. The data collected is then automatically processed and reported to HR departments in real-time. If a worker's responses indicate negative emotions or stress, the system may trigger an automatic referral to company-provided health resources, such as in-house therapists or counselling services. While these systems are often presented as 'wellness programs', they raise significant risks.[29]

Algorithmic management

The rapid pace of technological innovation has also set the stage for the rise of algorithmic management: the potential automation of the full range of traditional employer functions, from hiring workers and managing the day-to-day operation of the enterprise through to the termination of the employment relationship. First introduced in digital labour platforms,[30] algorithmic management systems have long outgrown their origins and have come to workplaces across the socio-economic spectrum, from factories, logistics centers, and warehouses to professional service firms, financial institutions, and media organisations.[31]

Algorithmic management systems can be used at all stages of the employment lifecycle, including in recruitment, work allocation, performance management, workers monitoring and dismissal. At the recruitment stage, algorithmic management systems are used to target job advertisements on social media sites, screen and rank applications, decide which applicants to invite to interviews, and evaluate candidates during interviews by analysing different aspects of communication.[32] According to the US Equal Employment Opportunity Commission, as many as 83% of employers, and as many as 90% among Fortune 500 companies have adopted algorithmic

[26] ibid.
[27] 'The Algorithm That Tells the Boss Who Might Quit...Wal-Mart, Credit Suisse Crunch Data to See Which Workers Are Likely to Leave or Stay' <https://www.firstsun.com/2015/03/18/strategy-the-algorithm-that-tells-the-boss-who-might-quit-wal-mart-credit-suisse-crunch-data-to-see-which-workers-are-likely-to-leave-or-stay/> accessed 30 March 2025.
[28] Ball (n 13).
[29] Expert Response India.
[30] Antonio Aloisi and Valerio De Stefano, *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour* (Hart 2022).
[31] 'Algorithmic Management in Traditional Workplaces' (*Foundation for European Progressive Studies*) <https://feps-europe.eu/publication/algorithmic-management-in-traditional-workplaces/> accessed 30 March 2025.
[32] Airlie Hilliard, Nigel Guenole and Franziska Leutner, 'Robots Are Judging Me: Perceived Fairness of Algorithmic Recruitment Tools' (2022) 13 Frontiers in Psychology 940456.

decision-making systems to rank applicants by scanning their CVs.[33] HireVue, a leading provider of software for vetting job candidates, claims that its algorithmic management systems can score job applicants based on their tone of voice, word choices, and facial expression captured during video interviews, though some of these systems have proven fundamentally unfit for purpose.[34] During employment relationships, algorithmic management tools could be used to replace or augment managerial functions, such as allocating tasks, the pricing of individual assignments, determining working schedules, giving instructions, evaluating the work performed, providing incentives, imposing sanctions, and even firing workers.[35] They can also be used to predict future behaviour of workers, such as whether workers will quit or try to organize a union, affecting employers' decisions about job assignment and promotion.[36]

The increasing deployment of algorithmic management systems could significantly affect working conditions and social relationships and pose significant risks to the privacy, human dignity, health and safety, equal treatment, and autonomy of workers. Algorithmic management systems also pose significant obstacles to worker mobilisation, unionisation, and collective action, especially in platform work. Instead of building a sense of community and solidarity, algorithmic management pits workers against one another, making building collective power difficult. While several regulatory measures are in the pipeline in many jurisdictions, they are still in a nascent stage.

Driving forces for the boom in workplace technologies

The increasing adoption of sophisticated surveillance and decision-making technologies in the workplace has been driven by a combination of socio-economic and technological factors. In this regard, it is possible to point to four broad trends that have contributed to the increasing datafication of work and the relentless quest for workers' data collection: advances in technology, reduced economic constraints, the shift to remote work, and the platformisation of work.[37] Each factor is briefly explained below.

The world of work has become the testing ground for sophisticated technologies for monitoring and controlling the behaviour of individuals. Intrusive monitoring and surveillance technologies are often used in the workplace before they are used in other contexts. As the European Fundamental Rights Agency (FRA) has noted, 'some of the most advanced technologies for monitoring and controlling the behaviour of individuals… are used predominantly in working life'.[38] Employers are increasingly deploying sophisticated technologies designed to collect vast quantities of data not just about what goes on in a workplace but also about what workers think and

[33] Jessica B Lee and others, 'A Privacy and Employment Law Primer: Recent Updates on Discrimination and Privacy Implications of Technology in the Workplace' (August 2022) <https://www.loeb.com/en/insights/publications/2022/08/recent-updates-on-discrimination-and-privacy-implications-of-technology-in-the-workplace> accessed 18 November 2024; James Hu, '99% of Fortune 500 Companies Use Applicant Tracking Systems' (*Jobscan*, 7 November 2019) <https://www.jobscan.co/blog/99-percent-fortune-500-ats/> accessed 1 October 2022; Eric Reicin, 'AI Can Be A Force For Good In Recruiting And Hiring New Employees' (*Forbes*, 16 November 2021) <https://www.forbes.com/sites/forbesnonprofitcouncil/2021/11/16/ai-can-be-a-force-for-good-in-recruiting-and-hiring-new-employees/> accessed 1 October 2022.

[34] Alene Rhea and others, 'Resume Format, LinkedIn URLs and Other Unexpected Influences on AI Personality Prediction in Hiring: Results of an Audit', *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society* (ACM 2022) <https://dl.acm.org/doi/10.1145/3514094.3534189> accessed 8 November 2024.

[35] Colin Lecher, 'How Amazon Automatically Tracks and Fires Warehouse Workers for "Productivity"' (*The Verge*, 25 April 2019) <https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations> accessed 12 November 2024.

[36] Kung Feng, 'Overview of New Rights for Workers under the California Consumer Privacy Act' (*UC Berkeley Labor Center*, 6 December 2023) <https://laborcenter.berkeley.edu/overview-of-new-rights-for-workers-under-the-california-consumer-privacy-act/> accessed 23 March 2025.

[37] 'Algorithmic Management in Traditional Workplaces' (n 34).

[38] European Fundamental Rights Agency, 'Data Protection in the European Union: The Role of National Data Protection Authorities' (Publications Office of the European Union, 2010) 37.

feel. Recent technological breakthroughs in machine-learning, big data analytics, and biometrics have significantly expanded capacities for worker surveillance both on and off the job. According to the European Commission's report, a wide range of new technologies have enabled workplace monitoring and surveillance that 'extend beyond the realm of performance management and into the thoughts, feelings and behaviours, location and movement, and professional profile and reputation of the employee'.[39] These technologies make more aspects of workers' lives visible to managers through data and provide employers with novel data sources, insights, and control mechanisms, enabling worker monitoring at unprecedented levels of detail, speed, and scale.

Concurrent with these technological advancements is the decrease in procurement, implementation, and maintenance costs, making even the most advanced workplace monitoring and decision-making technologies affordable for employers. In the past, purchasing, maintaining, and using workplace monitoring and surveillance systems often involved considerable expense.[40] That is not the case anymore; 'big data, algorithms and artificial intelligence now allow employers to process information on their workers and potential workers in a far more efficient manner and at a much lower cost than in the past.'[41] The decreasing cost of purchasing sophisticated technologies, coupled with the ease with which a vast amount of data is being collected and processed, further encourages employers to resort to more intrusive monitoring practices beyond a clearly defined legitimate purpose.

In addition to the decreasing economic constraints and increasing sophistication of technology, the rise of remote and hybrid work, accelerated by the COVID-19 pandemic, has further fuelled the demand for workplace monitoring and automated decision-making technologies.[42] Industry and media reports show that the global demand for workers monitoring technologies grew to new heights during the pandemic and continues to grow with no sign of slowing.[43] The trend towards remote work, which makes the work-private life boundary a contested terrain, has led to more pervasive and intrusive surveillance practices. As remote work becomes more prevalent, workers are increasingly accepting monitoring as a trade-off for flexibility.[44]

Lastly, the emergence of a new form of organizing work − platform work− has added new dimensions to workplace monitoring and surveillance. Platform work, which inherently involves algorithmic management and is characterized by an 'end-to-end employee surveillance', allows the collection of vast amounts of data on performance, behaviours and location and combined with customer feedback to determine algorithmically what work and reward are offered to the platform worker in the future.[45]

The convergence of these factors − the increasing sophistication and affordability of technology, the rise of remote and hybrid work, and the platformisation of work − is reshaping the landscape of workplace surveillance practices and decision-making. However, these developments have not been accompanied by the creation of appropriate regulatory responses. As this trend

39 Ball (n 13).
40 'The Electronic Supervisor: New Technology, New Tensions' (n 9).
41 Adrián Todolí-Signes, 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection' (2019) 25 Transfer: European Review of Labour and Research 465.
42 Polly Mosendz and Anders Melin, 'Bosses Are Panic-Buying Spy Software to Keep Tabs on Remote Workers' (*Los Angeles Times*, 27 March 2020) <https://www.latimes.com/business/technology/story/2020-03-27/coronavirus-work-from-home-privacy> accessed 23 October 2024; Eurofound (n 5).
43 Ball (n 13).
44 Riso (n 10).
45 Fernandez Macias, E., Urzi Brancati, M.C., Wright, S. and Pesole, A., The platformisation of work, EUR 31469 EN, Publications Office of the European Union, Luxembourg, 2023, ISBN 978-92-68-01661-9, doi:10.2760/801282, JRC133016. Rani, U., Pesole, A. and Gonzalez Vazquez, I., *Algorithmic Management practices in regular workplaces: case studies in logistics and healthcare*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2760/712475, JRC136063.

continues, it will be crucial to address the implications for workers' fundamental rights, including privacy and data protection rights, dignity, autonomy, and health and safety.

▶ 2 The risks for workers' fundamental rights and interests

When properly implemented and well-regulated, workplace technologies can offer substantial benefits for workers, employers, and society in general. They can facilitate skills development and on-the-job learning, 'enhance workers' safety (particularly in hazardous or emergency situations) and improve productivity and overall working conditions.[46] However, if left unregulated or poorly managed, the digitalization of the world of work can pose significant risks to workers' rights and well-being.

The potential dangers of unregulated workplace technologies are multifaceted and there is no simple term of analysis. The risks vary across industries and depend on a wide range of factors. As noted in the 1987 US Office of Technology Assessment report, 'whether the effect of monitoring is perceived as intrusive, unfair, dehumanizing, or unhealthy often depends on how management structures the work-monitoring program, what it does with the data it collects, and how those actions are perceived by employees.'[47] Following along these lines, Daniel M. Ravid and others developed a framework to understand the effects and implications of new monitoring and surveillance technologies.[48] According to the authors, the risks of workplace monitoring and surveillance technologies could be affected by four factors, which can be summarised as follows.

1. The **Purpose** for which the technology is used: Ravid and others argue that different workplace monitoring, and surveillance purposes communicate different organisational values.[49] For instance, 'if used constructively, performance monitoring may increase motivation, task satisfaction, dedication and perceptions of procedural justice; if used punitively the opposite happens'. Similarly, 'where there is no explicit purpose, and information is collected for its own sake, monitoring can result in negative attitudes, including perceptions of decreased fairness and justice perceptions, decreased satisfaction and increased stress with negligible impact on performance'.[50]
2. The relative **intrusiveness** of the technology used: The intrusiveness of a workplace technology depends on the *scope, target*, and *constraints* of the technology used and the extent affected workers have *control* over the technology and practice. The scope of monitoring implicates how much of a worker's task is monitored and the number of ways the worker is monitored or the degree to which the data collection is individualized. For instance, the specific form of electronic monitoring could be considered less intrusive if it is limited to the smallest number of workers and collects the least amount of data necessary to accomplish a clearly defined legitimate purpose. Similarly, the target refers to the intimacy or personal nature of the monitoring, which depends on the focus and kinds of information collected.[51] The third element that can affect intrusiveness is the degree to which there are explicit constraints on when and how the monitoring takes place and how will have access to the data collected. Lastly,

46 Sara Riso, 'Monitoring and Surveillance of Workers in the Digital Age' (Eurofound) <https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age> accessed 3 October 2024.
47 'The Electronic Supervisor: New Technology, New Tensions' (n 9).
48 Ravid and others (n 16).
49 ibid.
50 ibid.
51 ibid.

the extent to which the workers affected by the monitoring have control over when and how the monitoring takes place significantly affects the intrusiveness of workplace technology.

3. The **synchronicity** of monitoring: This factor refers to the temporal characteristics of workplace monitoring, including frequency and regularity of monitoring. For instance, continuous, real-time or covert monitoring systems could have more negative outcomes compared to intermittent and targeted monitoring.
4. The **transparency** of monitoring: The extent to which workers are provided with information about the characteristics of monitoring affects legitimacy of workplace monitoring and decision-making technologies. In this regard, Ravid and others argue that there are relatively strong positive relationships between transparency and workers' attitudes, including perceptions of fairness and justice in the workplace.

This framework underscores that the regulation of workplace technologies inherently requires the balancing of competing values: the legitimate interests of the employer and the fundamental rights and freedoms of workers.

Privacy and data protection risks

As highlighted above, employers collect personal data on job applicants and workers and there are several legitimate grounds to do so. Some of these legitimate grounds include to comply with law; to assist in selection for employment, training and promotion; to organize work; and to ensure personal safety, personal security, quality control, customer service and the protection of property.

While employers have a range of legitimate interests to monitor their workforce and utilise new technologies to do so, such practices cannot reduce the privacy and data protection rights of workers to zero.[52] As the Article 29 Working Party put it '[Workers] do not abandon their right to privacy and data protection every morning at the doors of the workplace.'[53] In other words, they expect that their workplace privacy and data protection rights are balanced with the employer's legitimate interests.

Therefore, as in any other context that involves the processing of personal data, the core challenge in regulating workplace technologies lies in creating this fair balance. While personal data processing in any context often involves inherent tension between competing legitimate interests, and striking the right balance is the primary objective of data protection and privacy laws, the employment context is distinct from other data processing activities in the digital world. This distinction gives rise to unique challenges and requires a fundamental rethinking of existing rules. There are several features that make the processing of personal data in employment settings distinct form other contexts, leaving workers more exposed. Some of the distinct features include:

The nature of data processed: Employers collect vast amount of sensitive data about their workers, often monitoring every aspect of their lives and movements across different devices. This extensive and intimate data collection creates significant privacy harms that go far beyond violations of existing legal rights to privacy and data protection. Beyond performance, the monitoring can focus on workers' thoughts, feelings, physiology, body and behaviour. Algorithmic management systems exacerbate this issue as they rely on vast amount of data to learn patterns and make inferences, predictions, recommendations, and decisions about workers. These systems

[52] *Bărbulescu v Romania* [2017] ECtHR 61496/08 [80].
[53] Article 29, 'Working Document on the Surveillance of Electronic Communications in the Workplace, 5401/01/EN/Final' (2002).

require constant data input from workers to function effectively. This comprehensive data collection and the sensitive nature of the data collected raise legal questions that may not have an explicit answer in general data protection regimes.

The routine nature of data collection: While various aspect of our private and public lives in the digital age are routinely tracked, it would be a misconception to view workplace monitoring and surveillance as merely an extension of this ubiquitous data collection.[54] The monitoring and surveillance practices in employment settings is fundamentally different, characterised by a persistent and intrusive approach to data gathering. Unlike the sporadic and transactional nature of data collection in other contexts, many activities performed routinely in the workplace often entail continuous observations of workers' activities and behaviour through data.[55] The ongoing nature of this data collection and processing is inherent to the employment setting, where various aspects of workers' lives are regularly monitored and analysed over an extended period.[56] The extensive nature of data collection is an essential consequence of the employment relationship from which workers cannot escape. It begins even before the employment relationship is established, persists throughout the employment period, and can continue even after the relationship has ended. This continuous data flow creates a comprehensive profile of the worker, raising significant privacy concerns and necessitating careful consideration of data protection and privacy measures in the workplace.

Blurred boundaries: Privacy in the workplace raises complex legal issues, particularly when business-related information and the personal data of workers are deeply intertwined, which is often the case. Interpreting broadly Article 8 of the European Convention on Human Rights (right to respect for private life), the European Court of Human Rights (ECtHR) explored the difficulty in clearly separating an individual's professional and personal life. In *Niemitz v. Germany*, the Court held that:

> *Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that (...) it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time. To deny the protection of Article 8 on the ground that the measure complained of related only to professional activities (...) could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them.*[57]

[54] Claire EM Jervis, 'Barbulescu v Romania: Why There Is No Room for Complacency When It Comes to Privacy Rights in the Workplace' (*EJIL: Talk!*, 26 September 2017) <https://www.ejiltalk.org/barbulescu-v-romania-why-there-is-no-room-for-complacency-when-it-comes-to-privacy-rights-in-the-workplace/> accessed 22 March 2025.

[55] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context (WP 48) 13 Sept 2001.

[56] EM Jervis (n 57).

[57] ECtHR, *Niemietz v Germany* (1992) Para 29.

Furthermore, employers' use of new technologies may not only affect privacy in the workplace, but also has the potential to blur the distinction between a workers' activities at work and their private lives. This is particularly evident in the context of remote and hybrid work, in which monitoring and surveillance technologies can reach beyond the work environment into workers' personal lives creating an even greater impact on workers' privacy.[58]

Nature of the relationship: The nature of the employment relationship is distinct from other commercial relationships, in at least in two aspects. First, the employment relationship inherently involves a power dynamic not present in many other data processing contexts. This relationship of power and of control goes beyond the traditional controller–data subject relationship underpinning modern data protection laws. Compared to the relative freedom- however limited- that consumers may have to choose the type of service or technology they use, workers do not decide what technologies should be deployed in the workplace and how these technologies should be used. The power to do so is the employer's prerogative. Consequently, workers may be considered as a sort of 'captive population' in regard to the use of data processing techniques.[59]

This power relation directly challenges some of the key underlying principles of data protection law, such as consent. The inherent inequality of power allows employers to control not only the work but also the physical and mental well-being of their workers.[60] As the European Data Protection Board (EDPB), recently noted, the employment relationship requires an assessment that is different from the one concerning a service provider-customer relationship because of the status of the employer vis-à-vis the workers.[61]

The second aspect is the personal nature of the relationship, which is presumed to be built on mutual trust and confidence. This nature was succinctly summarised by the UK Lord Justice of Appeal, Lord Justice Mummery, in *Keen v Commerzbank AG:* 'Employment is a personal relationship. Its dynamics differ significantly from those of business deals and of state treatment of its citizens. In general, there is an implied mutual duty of trust and confidence between employer and workers. Thus, it is the duty on the part of an employer to preserve the trust and confidence which an employee should have in him.'[62]

The element of trust in employment relations inherently entails the risk that the employer could abuse such trust. This risk becomes particularly salient in the context of automated decision-making systems. Reflecting on how these technologies can affect the personal nature of the employment relationship and impact the human dignity of workers, Robin Allen and Dee Masters argue that 'the increased reliance on technology to make management decisions risks profoundly undermining the personal nature of the employment relationship'.[63] They further contend that 'where human involvement is lacking and the expectations of employees by their employers become more and more a matter of digitised targets, the role of the employee is increasingly diminished'. Therefore, the increasing reliance on algorithmic decision-making systems raises important questions about the preservation of trust, respect, and human dignity in the workplace. As employers increasingly rely on AI systems for decision-making, there is a risk of depersonalizing the employment relationship (datafication of workers), potentially eroding the mutual trust

58 Article 29 Working Party Opinion 2/2017 on data processing at work (WP 249) 8 June 2017.
59 Council of Europe Explanatory Memorandum to Recommendation No. R (89) 2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes (Adopted by the Committee of Ministers on 18 January 1989).
60 Halefom H Abraha, 'A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace' (2022) 12 International Data Privacy Law 276.
61 Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0 Adopted on 8 October 2024).
62 Keen v Commerzbank AG [2006] EWCA Civ 1536 https://www.iclr.co.uk/document/2016062679/2006ewcaciv1536_TNA/html.
63 Robin Allen and Dee Masters, 'Technology Managing People—The Legal Implications' (Trades Union Congress 2021).

and confidence that labour law seeks to preserve. Furthermore, intrusive and unjustified monitoring and surveillance of workers violates this implied trust and confidence as such practices could come from presumption of the workers' misbehaviour.[64]

The nature of interests at stake: In contrast to what modern privacy and data protection laws envisage, the privacy and data protection issues that arise within the employment context are both individual and collective. Workplace monitoring and surveillance can affect not just an individual worker but the workforce as a whole within the enterprise. Privacy harms in the workplace arise not just from the processing of an individual's personal data in isolation, but from the analysis of relationships, patterns, and correlations across large datasets. For instance, to predict unionisation activities, employers do not need to monitor the behaviour of an individual worker as they can infer this from data about others.[65] Privacy harms in the workplace are caused collectively and felt collectively and cannot be adequately addressed by individualistic data protection laws. Most existing data protection laws are individualistic in nature, making them inadequate to deal with the inherently collective rights and interests of workers.

Relational nature of risks: As the European Data Protection Working Party observed, not all problems that arise in the employment context and involve the processing of personal data are exclusively data protection ones.[66] As discussed below, the risks posed by new workplace technologies are not confined within the privacy and data protection rights alone. These risks are multifaceted affecting multiple interests and values simultaneously. In June 2020, the European Social Partners released a Framework Agreement on digitalization in which they found a common ground on the fact that the use of digital technologies and AI surveillance systems in the workplace raise new risks of compromising human dignity and contributing to a deterioration of working conditions.[67]

Beyond privacy and data protection

Privacy and data protection are the often-cited concerns of pervasive workplace technologies. However, the impact of these technologies cannot be framed in terms of privacy and data protection alone. Monitoring and algorithmic management technologies engage not just with privacy and data protection issues but also affect broader social and labour rights enshrined in international and national laws.

For instance, the integration of workplace monitoring, surveillance technologies and algorithmic management systems poses significant risks to worker's autonomy, dignity, health and wellbeing. Extensive research highlights how productivity-tracking tools and machine-paced workflows contribute to physical and mental strain, with studies showing 74% of warehouse workers of a specific company avoiding bathroom breaks due to performance targets and 55% reporting depression.[68] These systems intensify workloads through algorithmically determined targets, real-time performance evaluations, and unpredictable scheduling, creating chronic stress and

64 Breen Creighton and Andrew Stewart, *Labour Law: An Introduction* (3rd ed) (2000)

65 Harmon Leon, 'Whole Foods Secretly Upgrades Tech to Target and Squash Unionizing Efforts' (*Observer*, 24 April 2020) <https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/> accessed 1 August 2024.

66 Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48.

67 'European Framework Agreement on Digitalisation' (BusinessEurope, SMEunited, CEEP and the ETUC 2020).

68 Darrell M West, 'How Employers Use Technology to Surveil Employees' (*Brookings*, 5 January 2021) <https://www.brookings.edu/articles/how-employers-use-technology-to-surveil-employees/> accessed 30 March 2025.

safety hazards.[69] One study shows that 87% of call centre workers surveyed reported high or very high stress levels at their work, with 50% of them reporting having been prescribed medication for stress or anxiety.[70] Data-driven technologies enable unprecedented micromanagement, reducing workers to dehumanized data points.[71] The Council of Europe warns that constant surveillance transforms workers into a 'captive population',[72] eroding dignity through statistical profiling and automated decision-making. This degradation of agency is compounded by invasive monitoring in private workspaces, which workers often perceive as demeaning. Paradoxically, excessive surveillance can backfire, fostering distrust, reducing job satisfaction, increasing turnover, and encouraging rule breaking.[73]

Algorithmic bias in hiring and management systems perpetuates systemic discrimination. Amazon's abandoned AI recruitment tool, which penalised resumes containing the word 'women', exemplifies how historical biases embedded in training data disadvantage protected groups.[74] Facial recognition and speech analysis tools show racial and gender biases, while automated assessments misinterpret physical or behavioural differences in disabled applicants.[75] Marginalised groups face compounded harms in low-wage sectors like warehousing, where invasive monitoring disproportionately affects women and people of colour. These technologies risk entrenching inequality by creating opaque barriers to employment opportunities.

Unionisation efforts face new threats from predictive surveillance systems and algorithmic management, potentially disrupting the delicate balance between labour rights and business interests that many legal systems have strived to maintain.[76] There have been reports of some US companies using machine learning to assign 'risk scores' to locations based on unionisation likelihood, analysing anonymised data to pre-empt labour organising, and even censor terms like 'unionise' in internal communications.[77] Platform workers are particularly vulnerable due to algorithmic management models that isolate them, foster competition, and eliminate physical gathering spaces. Some employers reportedly screen job candidates for union sympathies, effectively blacklisting labour rights advocates before hiring.

---

69 Michael Sainato, '"You Feel like You're in Prison": Workers Claim Amazon's Surveillance Violates Labor Law' *The Guardian* (21 May 2024) <https://www.theguardian.com/us-news/article/2024/may/21/amazon-surveillance-lawsuit-union> accessed 12 November 2024; Ariel Bogle, '"Stop All Time Wasting": Woolworths Workers Tracked and Timed under New Efficiency Crackdown' *The Guardian* (22 October 2024) <https://www.theguardian.com/business/2024/oct/23/woolworths-staff-efficiency-productivity-crackdown-timed> accessed 12 November 2024; Feng (n 39); United Workers Union, 'Technology and Power: Understanding Issues of Insecure Work and Technological Change in Australian Workplaces' (2020); Virginia Doellgast and Sean O'Brady, 'Making Call Center Jobs Better: The Relationship between Management Practices and Worker Stress' [2020] Cornell University, ILR School.

70 Doellgast and O'Brady (n 72).

71 Feng (n 39).

72 Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes 1989.

73 Melissa A Wheeler, 'Does Tracking Your Employees Actually Make Them More Productive?' (*The Conversation*, 24 October 2024) <http://theconversation.com/does-tracking-your-employees-actually-make-them-more-productive-242027> accessed 12 November 2024; Magan Nicole O'Neal, 'The Effects of Productivity Tracking on Employees' (*Indeed Career Guide*) <https://www.indeed.com/career-advice/career-development/effects-productivity-tracking-employees> accessed 12 November 2024.

74 Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women' *Reuters* (11 October 2018) <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/> accessed 23 October 2024.

75 Miranda Bogen, 'All the Ways Hiring Algorithms Can Introduce Bias' *Harvard Business Review* (6 May 2019) <https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias>; Meredith Whittaker and others, 'Disability, Bias, and AI - Report' (AI Now Institute 2019) <https://ainowinstitute.org/publication/disabilitybiasai-2019> accessed 9 November 2024.

76 Jamie Susskind, *The Digital Republic: On Freedom and Democracy in the 21st Century* (Pegasus Books 2022) 139; Grace Scott, 'Labor Organizing and AI Surveillance in the Workplace' (*George Town Journal on Poverty Law & Policy*, 14 January 2024) <https://www.law.georgetown.edu/poverty-journal/blog/labor-organizing-and-ai-surveillance-in-the-workplace/> accessed 12 November 2024.

77 Harmon Leon, 'Whole Foods Secretly Upgrades Tech to Target and Squash Unionizing Efforts' (*Observer*, 24 April 2020) <https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/> accessed 10 November 2024; Shirin Ghaffary, 'The Real Cost of Amazon' (*Vox*, 29 June 2020) <https://www.vox.com/recode/2020/6/29/21303643/amazon-coronavirus-warehouse-workers-protest-jeff-bezos-chris-smalls-boycott-pandemic> accessed 10 November 2024.

The automation of consequential decisions, such as termination, removes human accountability from employment relationships. In one case, an e-commerce company claimed local managers had no understanding or control over an algorithmic system that fired workers allegedly for union activities. This erosion of human agency leaves workers without recourse, as decisions requiring empathy or contextual understanding can be delegated to opaque algorithms. Legislative efforts to mandate 'human in the loop' in significant decisions reflect growing recognition that algorithmic judgments lack the nuance need for fair employment practices.

Lack of algorithmic transparency is another challenge. The opaque nature of many algorithmic systems, combined with corporate trade secrecy laws, exacerbates power imbalances between employers and workers.[78] Many workers are unaware of what data is collected, how it's processed, or even the existence monitoring tools.[79] Without meaningful transparency, workers cannot exercise their rights to explanation, contestation, or redress enshrined in some jurisdictions. Third-party vendors often control these systems, leaving employers themselves unable to fully explain or audit algorithmic outcomes. Jamie Susskind observes, 'sometimes the power of technology derives from the very fact that its workings are hidden',[80] underscoring how opacity entrenches employer dominance.

These issues collectively threaten labour rights frameworks designed to balance worker protections with business interests. The intensification of surveillance-driven productivity tracking metrics, opaque and biased automated decisions, suppression of collective action, and the lack of accountability mechanisms create a workplace environment where workers' autonomy and dignity are systematically undermined.

78 Alex Rosenblat and Luke Stark, 'Uber's Drivers: Information Asymmetries and Control in Dynamic Work' [2015] SSRN Electronic Journal <http://www.ssrn.com/abstract=2686227> accessed 22 November 2024.

79 WP 249, Opinion 2/2017; Jeremias Adams-Prassl and others, 'Regulating Algorithmic Management: A Blueprint' (2023) 14 European Labour Law Journal 124.

80 Jamie Susskind, *The Digital Republic: On Freedom and Democracy in the 21st Century* (Bloomsbury Publishing 2022) 219.

▶ 3 Existing protections

Global standards

The ILO and the Council of Europe have been pioneers in setting international standards on workers' data protection rights since the early 1990s. In 1991 and 1993, the ILO published two comprehensive reports on workers' privacy and monitoring and surveillance in the workplace.[81] After reviewing the then-existing regulations across several jurisdictions, ILO's 1991 report concluded that while they contained a series of general rules applicable to the employment context, most of the laws reviewed did not explicitly deal with the processing of workers' data.[82] The report found that consistent and comprehensive regulation on workers' data protection was missing at both international and national levels, and that international instruments were needed to bridge the gap. Specifically, since the 1990s, it appears that the ILO has maintained a clear stance that the general and abstract provisions of omnibus data protection laws are insufficient to deal with workers' data protection rights.[83]

The Council of Europe began the debate even earlier. After the adoption of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in 1981, the Council of Europe recognised that neither the broad principles of the Convention nor omnibus national data protection regulations could adequately regulate data processing in the employment context. Consequently, the Council then started exploring a sectoral regulation for workers' data protection rights in the early 1990s.

Unlike typical international rules that often aim to establish common standards based on existing national provisions, the ILO and the Council of Europe took a proactive approach in the absence of widespread national regulations in this field.[84] In 1989, the Council of Europe a Recommendation on the 'Protection of personal data used for employment purposes (revised in 2015), while the ILO adopted its Code of Practice twelve years later. Both organisations recognized the practical importance of rules on workers' data processing and viewed international instruments as a means to address the regulatory gaps. However, they chose less intrusive forms of regulation: the Council of Europe opted for a Recommendation, while the ILO selected a Code of Practice. This approach, while not legally binding, provided a framework for reflection and set expectations.[85] While the Recommendation appeals to Member States to incorporate its principles into domestic legislation on data protection in the employment sector, the Code of Practice aspires to serve as a guidance in the development of legislation, regulations, collective agreements, work rules, policies and practical measures at enterprise level. Consequently, these guidelines placed the discussion on a broad, solid basis, delineating the scope and essential elements of regulation. By choosing these forms over conventions, which often involve lengthy negotiations

81 'Workers' Privacy Part I-Protection of Personal Data' (n 2); 'Workers' Privacy Part II: Monitoring and Surveillance in the Workplace' (n 17).

82 'Workers' Privacy Part I-Protection of Personal Data' (n 2) 16.

83 See Preface, ILO code of practice on the Protection of workers' personal data 1997 [noting 'While various national laws and international standards have established binding procedures for the processing of personal data, there is a need to develop data protection provisions which specifically address the use of workers' personal data'].

84 Simitis (n 3).

85 ibid; Paul De Hert and Hans Lammerant, 'Protection of Personal Data in Work-Related Relations' (European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2013).

and compromises, both organisations aimed to reach effective solutions and participate in the international debate promptly.[86]

In terms of content, both instruments are quite comprehensive considering the time they were adopted. They share many similarities but also have some notable differences. Both instruments cover the entire employment lifecycle, including current and former workers, as well as applicants, in both private and public sectors. Both are also applicable to personal data processing by workers' representatives and employment agencies. However, while the ILO's Code of Practice addresses both manual and automated processing, the Council of Europe's Recommendation focuses primarily on automated processing. Regarding principles, both emphasise lawfulness, fairness, purpose limitation, data minimisation, and transparency.[87] They also provide for specific rights for workers, including the right of access, notice, rectification, and objection.

Notably, these standards address critical aspects of workplace monitoring and automated decision-making systems. Both instruments prohibit solely automated decision-making, though with varying degrees of strictness. The Code of Practice strictly prohibits solely automated decision, requiring automated decision-making systems be used only as an auxiliary means. The Recommendation, on the other hand, prohibits solely automated decisions only when they can have a significant effect on the worker and when the worker's views are not taken into consideration. They grant special status to sensitive data, such as information revealing sex life, political opinions or religious or other beliefs, or criminal convictions.

Additionally, both recognise the power imbalance in employment relationships, excluding consent as a legal basis for processing certain types of data. For instance, they prohibit the processing of genetic information, even with consent, unless explicitly authorised by national legislation – a stance more protective than some modern data protection regimes such as the GDPR.[88] While the Code of Practice is largely silent on the matter of health data, the Recommendation provides more detailed guidance on this topic. Conversely, the Code of Practice explicitly prohibits the processing of personal data concerning the worker's membership in a workers' organization or the worker's trade union activities, unless obliged or allowed to do so by law or a collective agreement. The Recommendation, however, does not address this issue.

Most importantly, the Code of Practice recognises that workplace data protection rules should be grounded in labour law principles. Acknowledging the fundamental nature of workers' rights and the inherent power dynamics of employment relations, the Code of Practice prescribes that workers' data rights are non-waivable[89] – a stance that contrasts with modern consumer-oriented data protection regimes.

The guidelines adopt a similar approach to digital monitoring and video surveillance. The Code of Practice states that data collected through electronic monitoring should not be the sole factor in evaluating worker performance nor should these systems be used to control the behaviour of workers. Similarly, the Recommendation strongly prohibits the use of digital monitoring and surveillance systems for the direct and principal purpose of monitoring workers' activity and behaviour. The Recommendation provides more detailed guidance on location tracking and biometric data use, which are not explicitly mentioned in the ILO Code of Practice. Lastly, both instruments emphasise the importance of collective rights and the role of workers' representatives,

86 Simitis (n 3).
87 For details on this, see Frank Hendrickx, 'Protection of Workers' Personal Data: General Principles' (ILO Working Paper 62 2022).
88 Article 9 of the GDPR allows the processing of genetic data based on explicit consent.
89 ILO Code of practice on the protection of workers' personal data 1997 para 5.13.

recommending consultation and information on workers' data processing and the introduction of new technologies.

While these instruments provide frameworks for reflection by recognising the unique features of the employment relationship, they remain, as their nomenclature suggests, mere non-binding guidance. Furthermore, it remains uncertain how these principles can be updated to address the nuances of AI-driven decision-making and monitoring in the workplace.

A case study of selected jurisdictions

Workers' data protection is governed by multiple legal domains including data protection legislation, labour law, equality law and various sectoral or issue-specific laws. In many jurisdictions, workplace data rules are shaped not primarily by data protection and privacy legislation but by the influence of other sectoral laws. This highlights the need for an interdisciplinary approach to data governance that integrates these seemingly distinct legal domains to ensure effective protection of workers' data. This section explores the existing regulatory frameworks of selected jurisdictions, focusing on privacy and data protection legislation, labour and industrial relations rules, algorithmic management rules, and non-legislative regulations and guidelines. While insights from other jurisdictions such as India, China, Brazil, and several African countries are considered, the analysis primarily focuses on the EU, United States[90], and Australia due to their recent regulatory initiatives and the unique perspectives they offer in illustrating challenges and gaps in existing laws governing workers' data. It is important to note that this analysis highlights key regulatory frameworks and initiatives but does not claim to provide an exhaustive or fully comprehensive evaluation of all relevant instruments.

The European approach

A. Privacy and data protection legislation

The processing of personal data in the employment context has been subject to ongoing debate in Europe, at both the Union and national levels, predating the GDPR. The EU and several Member States have long recognised the need for workplace-specific data protection rules to make the broad principles of general data protection laws meaningful to the employment context, considering the unique requirements and special nature of employment relationships.

The German State of Hessen was not only the first to adopt the world's first data protection law, but it also pioneered the incorporation of special provisions exclusively applicable to data processing in the employment context.[91] This could be attributed to the influence of the late Spiros Simitis, a pioneer in the field of data protection in Europe and beyond. Simitis authored the Hessian data protection law and served as its Chief Data Protection Commissioner. He was a member of the Council of Europe's Data Protection Experts Commission and the European Commission's committee that developed the 1995 Data Protection Directive. Simitis also served as advisor to the ILO on creating a system for regulating workers' data protection, which led to the adoption of the 1997 Code of Practice. Simitis consistently argued that the then-existing omnibus frameworks for data protection laws, which he helped establish, were not designed to regulate workers' data processing. He advocated for the establishment of employment-specific data protection

[90] It's important to note that this report focuses on regulatory developments prior to the new Trump administration, thus some highlighted initiatives may have changed.

[91] 'Workers' Privacy Part I-Protection of Personal Data' (n 2) 16.

rules that take the distinct nature of the employment relationship into account.[92] Consequently, Simitis was pivotal in incorporating detailed rules on the processing of workers' data into the revised data protection legislation in Germany. Several Member States have subsequently included workplace-specific provisions into their respective data protection laws, with Finland being the only EU Member State to adopt comprehensive legislation targeted specifically at protecting personal data used for employment purposes.

At the Union level, the European Commission has made several efforts to introduce a workplace-focussed data protection framework since 2001. The Commission initiated consultations on the possibility of introducing a specific legislation on protection of workers' personal data in 2001 and 2004. While the Commission believed that a European framework was 'needed aiming at the protection of workers' personal data while striking a balance between the employer's legitimate interests and the workers' right to privacy', these initiatives were abandoned for lack of consensus among stakeholders.[93] Specifically, employers' organisations dismissed the proposed framework as 'premature', arguing that the then existing omnibus data protection legislation (Directive 95/46/EC) was 'adequate and sufficient to ensure high-quality protection of workers' personal data'.[94]

A similar effort between 2012 and 2018, during the GDPR's development and finalisation, to incorporate 'detailed and harmonised rules for the employment relationship' as part of the GDPR met the same fate.[95] Notably, the proposal included, among other things, (i) detailed rules on the 'proportionality and legitimacy' requirements of personal data processing in the employment context, (ii) the exclusion of consent as a valid legal basis for the processing of workers' personal data, and (iii) the provision of a delegated power to the Commission to provide for specific rules for the purpose of further specifying the criteria and requirements for the safeguards of workers' personal data. None of these proposals were ultimately incorporated into the GDPR, primarily due to the diverging views of social partners, lack of priority, and political compromise.[96] Therefore, while the inadequacy of omnibus data protection regimes to address the distinct features of workers' data processing and the necessity for sector-specific regulation have been long recognised, legislative efforts to introduce workplace-specific data protection law in the EU have been largely unsuccessful.

One of the key factors that makes it complex for the EU to harmonise the protection of workers' personal data is the overlapping constitutional powers to legislate on industrial relations, coupled with diverse traditions that exist among Member States regarding the regulation of employment relations.[97]

Following the entry into force of the GDPR in 2018, the EU provides some of the strictest privacy and data protection compared to other jurisdictions. The Charter of Fundamental Rights of the European Union elevates the right to protection of personal data to a constitutional status and

92 For similar account by other scholars, see Freedland (n 3).

93 European Commission, 'Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data' (2002); For more details on this, see Abraha, 'A Pragmatic Compromise?' (n 1).

94 European Commission, 'Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data' (2002); UNICE, 'Commission's Second-Stage Consultation on the Protection of Workers' Personal Data' (6 January 2003).

95 European Commission, 'Staff Working Document SEC(2012) 72 Final' 17, 111.

96 Abraha (n 63).

97 According to Article 153(1) of the Treaty on the Functioning of the European Union (TFEU), the EU has only 'supporting competence' in several aspects of employment matters. This is particularly true with regard to the collective aspects of labour law such as co-determination rights.

the GDPR gives effect to this right. The GDPR is widely regarded as the most advanced, comprehensive, and rights-based piece of legislation, with significant influence worldwide.[98]

The GDPR establishes a set of data protection principles and exhaustive legal bases that organisations should follow, embedding transparency and accountability frameworks. For employers, the most relevant legal bases are 'necessity for contract performance', 'legitimate interest', and 'consent'.

The GDPR also provides rights to data subjects whose personal data is being processed, with the purpose of giving them control over their data. These rights are applicable to workers as well. The obligation of transparency, enshrined under Article 5(1(a) of the GDPR and further elaborated under Articles 12-15, is regarded as 'a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data.'[99] The transparency obligations can enable workers to have a say in the processing of their personal data 'ex ante' and provide 'ex post' means for remedy, such as the right to rectification, erasure, objection to the processing.[100]

Article 22 of the GDPR provides a set of individual rights in automated decision-making including the right to obtain human intervention, the right to express one's point of view, the right to contest the decision, and the right to obtain an explanation. These rights, along with the right of access, have been instrumental in challenging monitoring and algorithmic management practices in the workplace, particularly in platform work.[101] The GDPR's transparency framework can be used to shed light on the inner workings of these AI algorithms, demystifying their complexity and allowing for scrutiny and accountability. The impact assessment regime under Article 35 GDPR is one of the key accountability requirements, which could play a crucial role in identifying and addressing the risks posed by digital monitoring and algorithmic management tools in the workplace. Ideally, algorithmic impact assessment in the workplace would involve workers or their representatives.[102]

However, while the GDPR remains crucial in taming some of the serious risks of workplace technologies, it suffers from significant 'structural deficits'[103] in addressing the unique features and complexities of the workplace. The legislation is of general in nature and does not contain employment sector specific provisions. Consequently, it is not sufficient to address the privacy and data protection issues that arise from the unique requirements and special nature of the employment relationship.

The GDPR itself recognises this limitation. Acknowledging the special nature of personal data processing in the employment context, the GDPR grants Member States regulatory leeway to

98 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford Scholarship Online 2020).

99 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions– A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final 6.

100 For details on the ex-ante information obligations of the controller and ex post rights of the data subjects, see Halefom Abraha, 'Regulating Algorithmic Employment Decisions through Data Protection Law' (2023) 14 European Labour Law Journal 172.

101 *Rechtbank Amsterdam, Case C/13/687315 / HA RK 20-207, ECLI:NL:RBAMS:2021:1020, March 11, 2021*; 'Employee Monitoring: CNIL Fined AMAZON FRANCE LOGISTIQUE €32 Million' <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> accessed 18 November 2024; Sebastião Barros Vale and Gabriela Zanfir-Fortuna, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities' (Future of Privacy Forum 2022); Christina Hießl, 'Jurisprudence of National Courts in Europe on Algorithmic Management at the Workplace' (European Centre of Expertise in the field of labour law, employment and labour market policies (ECE) 2023).

102 Article 35(9), GDPR.

103 Einat Albin, 'The Three-Tier Structural Legal Deficit Undermining the Protection of Employees' Personal Data in the Workplace' (2024) 45 Oxford Journal of Legal Studies 81.

introduce specific and more protective rules in this area, through the opening clause stipulated under Article 88(1) of the GDPR.

> *Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.*

This provision recognises that workers' data protection is a unique sub-field of data protection law and that the GDPR alone is not adequate to regulate this specific domain. It acknowledges the role of social partners in establishing workplace data protection rules and stipulates that these 'specific rules' shall include suitable and specific measures to safeguard the worker's human dignity, legitimate interests and fundamental rights. This approach suggests that workplace data protection laws should be designed with workplace relations in mind, based on labour law principles and standards rather than the consumer-oriented rules of general data protection law.[104] Consequently, the GDPR was designed under the assumption that data processing for employment purposes will be regulated by a different set of rules implemented alongside it.

Several Member States have notified the Commission that they have maintained or introduced workplace-specific data protection rules. These specific rules are incorporated into omnibus data protection laws or are other specific laws. For example, 22 Member States have specific provisions regulating workers monitoring and surveillance to some extent.[105] However, these laws are limited in scope and breadth.

A closer look at these Member states laws[106] and the CJEU and national court's decisions reveals that Member States have not yet fully taken the opportunity created under Article 88 of the GDPR. On 30 March 2023, the CJEU issued its first ruling on the interpretation of Article 88, in response to a request from the Administrative Court of Wiesbaden (*Case C-34/21*).[107] The court established that for national laws to qualify as 'more specific rules' under Article 88(1), they must: (1) be consistent with the GDPR's objectives of protecting workers' fundamental rights, (2) contain normative content distinct from the general GDPR provisions, and (3) include suitable and specific measures as required by Article 88(2), such as safeguarding human dignity and transparency in workplace monitoring. The Court found that German employment data protection rules, specifically Section 23 of the Hessian Data Protection Act and Section 26 of the Federal Data Protection Act, merely repeated GDPR provisions without adding substantive, sector-specific safeguards, and thus failed to meet these criteria.

This was followed by the German's Federal Labor Court decision on May 9, 2023, declaring Section 26 Para.1 of the Federal Data Protection Act (BDSG), which deals with data processing in the employment context, invalid and inapplicable, as it did not meet the requirements of Article 88 of the GDPR.[108] These decisions effectively invalidate key aspects of German's employment data protection framework, necessitating the introduction of a new legislative proposal, the Employee Data

104 ibid.

105 'European Restructuring Monitor: Employee Monitoring and Surveillance' (*Eurofound*) <https://apps.eurofound.europa.eu/legislationdb/employee-monitoring-and-surveillance> accessed 18 November 2024.

106 Abraha (n 63).

107 Case C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums* [2023] Digital Reports.

108 'Decision of May 09, 2023 – 1 ABR 14/22' (*Das Bundesarbeitsgericht*, 9 May 2023) <https://www.bundesarbeitsgericht.de/entscheidung/1-abr-14-22/> accessed 2 October 2024.

Protection Act 2024.[109] The CJEU's decision has wider implications across the Union, specifically for Member States with similar data protection laws. When considered in light of the CJEU's decision, most of the domestic rules on workplace data protection would most likely fail to meet Article 88 requirements. The decisions also justify the persistent calls for workplace-specific data protection laws.

B. Labour law and other legislative rules

In addition to the GDPR and national data protection laws, the protection of workers' personal data could be subject to other fields of law, particularly industrial relations legislation. For instance, at the Union level, Directive 2002/14/EC establishes the right of workers' representatives to be informed and consulted about substantial changes to work organisation and working conditions.[110] The introduction of devices designed to monitor the behaviour or performance of workers is considered a 'substantial change to work organisation' in some Member States including Austria, Germany, Finland, France and the Netherlands. This classification grants information and consultation rights to workers' representatives on matters of worker monitoring.[111]

Despite variations in scope and substance, several Member States have incorporated workers' data processing provisions in their respective labour laws. Some of these laws also allow the involvement of workers' representatives, such as works councils, to play a role in the protection of workers' personal data, though the degree of involvement varies across member states. In Countries like Austria, Germany, Sweden, and Italy, works councils or workers' representatives have agreement or co-determination roles regarding the introduction and use of new monitoring technologies. In contrast, member states like France and Finland limit this role to consultative or participatory functions.[112] Many other Member States either lack works councils or such councils have minimal involvement in data protection matters.[113]

The German and Austrian labour systems stand out for granting extensive rights to works councils in protecting workers' personal data. In Germany, the Works Constitution Act (BetrVG) requires companies which have more than five full-time workers to allow for the establishment of works councils.[114] These works councils have general responsibility to ensure the implementation of statutory instruments, including data protection and collective agreements.[115] They exercise a 'watchdog role'[116] through co-determination, participation, consultation, and information rights. German works councils have 'the right to be informed about most aspects of the employer's operations' and can veto decisions in certain situations.[117] For instance, the introduction of new technologies designed to monitor behaviour or performance requires a 'works agreement' between the employer and the works council. Similarly, the Austrian Labour Constitution Act grants works councils co-determination, participation, consultation, and information rights over

---

109 Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes 2024; 'Germany Draft for Employee Data Act Issued' (*www.hoganlovells.com*, 29 October 2024) <https://www.hoganlovells.com/en/publications/germany-draft-for-employee-data-act-issued> accessed 24 March 2025.

110 Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community - Joint declaration of the European Parliament, the Council and the Commission on employee representation.

111 Sara Riso and Chiara Litardi, 'Employee Monitoring: A Moving Target for Regulation' (*Eurofound*, 15 July 2024) <https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation> accessed 18 November 2024.

112 For more details on this, see Eurofound, 'Employee Monitoring and Surveillance: The Challenges of Digitalisation' (Publications Office of the European Union, Luxembourg, 2020).

113 Justin Nogarede, 'No Digitalisation without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace' (FEPS Policy Study, November 2021) 28.

114 Works Constitution Act 1972 (BetrVG) s 1.

115 ibid 80(1)1.

116 Robert G Schwartz Jr., 'Privacy in German Employment Law' (1992) 15 Hastings Int'l & Comp. L. Rev 151.

117 ibid 152.

a wide range of issues with privacy and data protection implication[118] and the power to monitor compliance with legal provisions and collective agreements affecting workers.[119] Works councils in Austria also have veto powers over the introduction of new monitoring technologies that affect the human dignity of the worker. In contrast, French law provides workers' representatives a more limited, consultative role. While the Labour Code allows for the establishment of workers' representative bodies, they do not enjoy co-determination rights like their German and Austrian counterparts. Employers must inform and consult these bodies prior to making a significant decision affecting workers, but they are not legally bound to accept their recommendations.[120]

C. Regulating Algorithmic management

The EU has recently introduced two landmark laws, the AI Act and the Platform Directive, which will have a significant impact in shaping the design, deployment and use of algorithmic management systems in the workplace. While the AI Act has faced criticism for inadequately protecting human rights in general and workers' rights in particular, it's important to acknowledge the protections it does provide, albeit limited, in safeguarding workers from some risks posed by algorithmic management and automated decision-making systems. The risk-based regulatory approach and specific provisions of the AI Act offer at least five key employment-specific protections, which collectively aim to safeguard workers' rights and interests in the face of increasing AI implementation in employment contexts. First, the AI Act does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or from encouraging or allowing the application of collective agreements which are more favourable to workers.[121] Second, it requires workers' rights to be included in fundamental rights and risk assessments of AI systems.[122] Third, the AI Act mandates employers inform and consult workers or their representatives about the planned deployment of high-risk AI systems in the workplace.[123] Fourth, it bans the use of emotion recognition AI systems in the workplace.[124] Finally, the AI Act classifies all AI systems used in the workplace as 'high-risk', imposing strict requirements before they can be put in the market.[125]

The Platform Work Directive is another piece of legislation that provides robust protections against AI-driven harms. One of its objectives is to improve the protection of personal data in the platform work by promoting transparency, fairness, human oversight, safety and accountability in algorithmic management in platform work.[126] In this regard, it provides relatively robust data protection, for example, by setting red lines regarding processing of personal data related to emotional or psychological state, private conversations, biometric data, or the prediction of the exercise of fundamental rights, and processing of data to infer sensitive information such as trade union membership. Unlike the GDPR, these prohibitions are not subject to exceptions.[127]

---

118 Labour Constitution Act 1974 ss 89, 90, 91,92, 96.
119 ibid 89.
120 Code du travail, Art. L. 2312-38. Art. L2323-2
121 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), Art 2(11), Rec. 9.
122 ibid, Rec. 48.
123 ibid, Art. 26, Rec. 92.
124 ibid, Art 5(1)(f), Rec. 44.
125 ibid, Art. 6(2), Annex III(4), Rec. 57.
126 Proposal for the DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work 7212/24 ADD 1, Art. 1(1)(b).
127 ibid, Art. 7.

The Platform Directive also strengthens the data protection impact assessment (DPIA) requirements stipulated under Article 35 of the GDPR by classifying the processing of personal data of platform workers by means of automated decision-making systems as high-risk within the meaning of Article 35(1). This classification triggers mandatory DPIA which requires employers to seek the views of workers and their representatives and to disclose the result of DPIA to workers' representatives, a requirement non-existent in the GDPR.[128] Furthermore, the Directive clarifies and expands algorithmic transparency requirements. Unlike the GDPR, the information obligations under the Platform Work Directive are not limited to 'solely automated decision-making' but include all types of decisions supported or taken by automated decision-making systems. It sets out transparency requirements both at individual and collective levels. It empowers national competent authorities to request 'comprehensive and detailed information' at any time. Lastly, the Directive mandates systemic oversight of the design and use of AI algorithms and human review of individual decisions supported or taken by these AI algorithms.[129]

Although its scope of application is limited to 'Platform Work',[130] the Directive has significantly improved the safeguards provided under the GDPR and the AI Act and can be used as a blueprint for future legislation with broader scope covering traditional employment settings.

Several Member States have also introduced or are considering algorithmic management regulation, although the content and scope of these regulations vary across countries. The European Restructuring database shows that 12 Member States have rules requiring transparency of algorithms, mandating human intervention in certain cases, and providing individual workers access to personal data processed.[131]

D. Non-legislative regulations and guidelines

The first EU policy intervention on the issue of workplace data protection was the Article 29 Working Party's Opinion 8/2001, complemented by a 'working document' on surveillance and monitoring of electronic communications in the workplace.[132] This Opinion was subsequently amended in 2017 to align with the new requirements of the GDPR. The WP29's Opinion 2/2017 provides comprehensive guidelines for the legitimate use of new technologies in various workplace scenarios. It details suitable and specific measures to safeguard the human dignity, legitimate interest and fundamental rights of workers.[133] The Opinion establishes a set of principles, outlines a list of risks posed by new technologies, and provides a framework for proportionality assessments in several workplace situations. While the Opinion aims to harmonise the application of data protection rules in the workplace across the EU, it is important to note that it is not legally binding and cannot be directly enforced against employers. It only serves as a guidance document, offering interpretations and recommendations for best practices in workplace data protection. Interestingly, the European Data Protection Board (EDPB), which replaced the Working

128 ibid, Art. 8.
129 ibid, Art. 10, Art.11.
130 Art. 2(2) of the Directive defines 'Platform Work' as any work organised through a digital labour platform and performed in the Union by an individual on the basis of a contractual relationship between the digital labour platform or an intermediary and the individual, irrespective of whether a contractual relationship exists between the individual or an intermediary and the recipient of the service.
131 'European Restructuring: Monitor Algorithmic Management' (*Eurofound*) <https://apps.eurofound.europa.eu/legislationdb/algorithmic-management> accessed 18 November 2024.
132 Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48. Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace (WP55) 29 May 2002.
133 Article 29 Working Party Opinion 2/2017 on data processing at work (WP 249) 8 June 2017 9 [emphasis added].

Party when the GDPR took effect in 2018, has not yet officially endorsed Opinion 2/2017.[134] Nor has the EDPB issued any specific guidelines regarding workplace data protection.

In its recent Guidelines on processing of personal data based on Article 6(1)(f) GDPR (legitimate interest), the EDPB recognises that the 'employer-employee relationship will likely require an assessment that is different from the one concerning a service provider-customer relationship'.[135] While it is commendable that the EDPB acknowledges the distinct nature of the legitimate interest balancing test in the employment context, the guidelines fall short in providing clarification for application in this context and thus offers little practical help for employers and workers.

The United States' approach

A. Privacy and data protection legislation

The United States' approach to privacy and data protection has arguably been shaped by the 1977 Privacy Protection Study Commission's recommendations. The Commission advised against an omnibus approach, instead favouring sector-specific regulation. In the context of workers' privacy, the Commission recommended voluntary self-regulation.[136] This decision has led to a fragmented regulatory landscape, with no comprehensive federal privacy and data protection framework. Instead, the US relies on a patchwork of federal and state legislation and self-regulation guidelines, often targeting specific industries or issues. This fragmentation is particularly pronounced when it comes to workplace privacy law, as shall be discussed below.

Several efforts to introduce comprehensive federal data protection law and employment-specific laws failed. In 1987, the Office of Technology Assessment published a comprehensive report, 'The Electronic Supervisor', articulating the risks that workplace electronic monitoring posed to workers' privacy and other rights and freedoms.[137] The study recommended that lawmakers introduce specific federal legislation to address these concerns, which led to the introduction of the Privacy for Consumers and Workers Act in 1991 before the House of Representatives.[138] This ambitious legislative proposal would have been the first comprehensive workplace-focused privacy law had it been adopted. It aimed to impose substantive limitations on employer monitoring practices that could not be circumvented even with worker's consent, while offering workers procedural protections, including prior notification and access rights. The bill and subsequent efforts were unsuccessful.

In recent years, however, the privacy and data protection legal landscape in the US has begun to change rapidly with several legislative initiatives at both the federal and state levels. From 2023 to 2024 alone, more than six dozen federal privacy bills were introduced, most of which are sectoral.[139] The latest federal legislative effort is the 'American Privacy Rights Act' of 2024, a comprehensive bill which aims to afford Americans fundamental and enforceable data privacy rights, largely pre-empting the patchwork of state laws.[140] However, even if the bill were adopted into law, which remains unlikely, there is one significant omission− the bill explicitly excludes workers' data from its scope of application.

---

134 'Endorsed WP29 Guidelines' (*European Data Protection Board*) <https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en> accessed 29 March 2025.
135 Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0, Adopted on 8 October 2024).
136 'Personal Privacy in an Information Society' (n 9).
137 'The Electronic Supervisor: New Technology, New Tensions' (n 9).
138 S.3238 - Privacy for Consumers and Workers Act 102nd Congress (1991-1992).
139 iapp, 'US State Privacy Legislation Tracker: Introduced in the 118th Congress (2023-2024)' <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> accessed 12 November 2024.
140 H.R.8818 - American Privacy Rights Act of 2024, 118th Congress (2023-2024).

There are also workplace privacy-focused legislative bills, although it remains uncertain whether these bills will become law. The four bills intended to regulate some aspects of workplace privacy include the *Stop Spying Bosses Act, No Robot Bosses Act, Protecting Healthcare Employee Privacy Act,* and *Exploitative Workplace Surveillance and Technologies Task Force Act*.[141] For instance, the 'Stop Spying Bosses Act' of 2024 aims to prohibit, or require disclosure of, the surveillance, monitoring, and collection of certain worker data by employers.[142] This bill would mandate employers disclose comprehensive information about workplace surveillance practices to their workers, including job applicants. The disclosure must detail what data are collected, how, when and where it's collected, the storage location, purpose of use, as well as how such workplace surveillance affects any employment-related decisions. The bill also stipulates the timing, manner and procedures of disclosure. Additionally, the Exploitative Workplace Surveillance and Technologies Task Force Act aims to establish an interagency task force on employer surveillance and workplace technologies.[143]

The US state privacy law landscape has been equally rapidly evolving. Between 2018 and 2024 alone, nineteen US states have adopted comprehensive data privacy laws, with more likely to follow.[144] With the exception of California, however, these US state laws explicitly exclude the processing of workers' personal data from their scope of application including workers, employees, job applicants, independent contractors. California became the first state in 2023 to extend consumer-like privacy rights to job applicants, employees, and independent contractors. The California Consumer Privacy Act (CCPA), enacted in 2018, initially exempted workers' data from its core privacy protection due to concerns about operational complexity for employers and extensive lobbying by business. This exemption reflected the law's original focus on consumer transactions rather than employment relationships. However, the California Privacy Rights Act, which amended the CCPA in 2020, allowed these exemptions to expire on January 1, 2023, extending full privacy rights to workers. Prior to 2023, employers were not required to grant workers rights such as data access, deletion, or opt-out from data sales. The exemption's sunset arose from legislative inaction, as efforts to extend it failed in 2022, as well as the growing recognition of workplace privacy risk amid digital monitoring and algorithmic management.

B. Labour law and other sector-specific legislative rules

The National Labor Relations Act (NLRA) protects workers' rights to organise and engage in collective activities, prohibiting employers from using surveillance tools to interfere with unionization efforts, while also mandating transparency in reporting surveillance costs related to labor disputes. As highlighted below, the National Labor Relations Board warned that the use of workplace surveillance and automated decision making may run afoul of workers' exercise of their rights under NLRA.

Additionally, there are specific provisions and issue-specific laws that regulate workers' privacy and data protections. For example, several states have laws prohibiting audio or video recording in workers' locker rooms, restrooms, or changing areas.[145] The Illinois Biometric Information Privacy Act (BIPA) requires employers to provide notice and obtain consent when collecting biometric

141 Ibid.
142 H.R.7690 - Stop Spying Bosses Act, 118th Congress (2023-2024).
143 S.2440 - Exploitative Workplace Surveillance and Technologies Task Force Act of 2023, 118th Congress (2023-2024).
144 Jordan Francis, 'Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends' (FPF US Legislation Report 2024) <https://fpf.org/blog/fpf-unveils-report-on-the-anatomy-of-state-comprehensive-privacy-law/>.
145 See for instance, California Code, Labor Code - LAB § 435; West Virginia's Electronic surveillance Act, Sec 21-3-20; New York Consolidated Laws, Labor Law - LAB § 203-c.

information from workers.[146] Similarly, the Colorado Privacy of Biometric Identifiers and Data Act restricts the collection of workers' biometric data by employers, narrowly limiting permissible reasons for obtaining consent to such data.[147] Some states such as Connecticut, Delaware, and New York have also adopted laws limiting workers' email and telephone communication monitoring.[148]

Much of the workplace privacy protection in the US is derived not from data protection legislation, but from the influence of other sectoral laws.[149] Key legislation such as the Health Insurance Portability and Accountability Act (HIPAA), Americans with Disability Act (ADA), and the Genetic Information Non-discrimination Act (GINA) play crucial roles in safeguarding individual's medical and genetic data in the workplace. HIPAA mandates confidentiality of workers' health data from group plans, while the ADA and its state counterparts require employers to keep medical records and health-related information of workers confidential. GINA prohibits employment decisions, such as hiring and firing, based on genetic information, prohibits discrimination on the basis of genetic information in any aspect of employment decisions. It restricts employers from requesting, requiring or purchasing genetic information, and strictly limits the disclosure of genetic information.[150] State-level cybersecurity laws also extend data breach notification requirements to the workplace.

C. Regulating Algorithmic management

Artificial intelligence has received significant regulatory attention at both the federal and state levels, with at least 45 states having either enacted or proposed laws to regulate AI.[151] Many of these laws and proposals are either employment-focused or have general implications for the use of algorithmic management and automated decision-making in the workplace.

At the federal level, the proposed No Robot Bosses Act 2024 aims to prevent use of automated decision-making systems by employers for specific purposes.[152] The Biden Administration's White House's Blueprint for an AI Bill of Rights was a federal initiative which might have had significant implications for workplace AI use.[153] The Blueprint stated that automated systems with an intended use within sensitive domains, such as employment, should be tailored to the purpose, provide meaningful access for oversight, include training for any people interacting with the system, and incorporate human involvement in adverse or high-risk decisions. The blueprint, however, is now defunct.

At the state level, New York City has pioneered legislation governing the use of AI in employment decisions, requiring bias audits, mandating that the results of such audit be made public, and obliging employers to provide notice to workers about the use of such tools. California proposed the comprehensive Workplace Technology Accountability Act (AB 1651), which prohibits the use of algorithmic management to make predictions about a worker's behaviour unrelated

146 Illinois Biometric Information Privacy Act 2008.
147 HB24-1130-Concerning Protecting the Privacy of an Individual's Biometric Data.
148 For details on this, see Peter Stockburger, 'Privacy in the US Workplace – a Rapidly Changing Legal Landscape' (*DENTONS*, 16 February 2023) <https://www.dentons.com/en/insights/articles/2023/february/16/privacy-in-the-us-workplace-a-rapidly-changing-landscape> accessed 29 March 2025.
149 'Workplace Privacy in US Federal and State Laws and Policies | IAPP' (*IAPP*) <https://iapp.org/news/a/workplace-privacy-in-us-laws-and-policies> accessed 29 March 2025.
150 'Genetic Information Discrimination' (*US EEOC*) <https://www.eeoc.gov/genetic-information-discrimination> accessed 29 March 2025.
151 'US State-by-State AI Legislation Snapshot' (*BCLP*) <https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html> accessed 29 March 2025.
152 H.R.7621 - No Robot Bosses Act, 118th Congress (2023-2024).
153 Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, October 2022.

to essential job functions, worker's emotions, personality, or the likelihood of workers exercising their legal rights.[154] This ambitious bill, however, has not become law.

New York City's Local Law 144 (automated employment decision-making law), effective since January 1, 2023, restricts AI use in employment decisions unless employers take certain actions regarding the use of AI tools. The law targets any automated management tools that substantially assist or replace discretionary decision making in screening job applicants for employment or promoting workers.[155] Illinois enacted the Artificial Intelligence Video Interview Act in 2020, regulating how employers can use AI and automated decision-making systems to analyse video interviews of job applicants.[156] Additionally, the state passed HB 3773 in 2024, amending the Illinois Human Rights Act. Effective as of January 2026, this law will prohibit AI use in a manner that results in illegal discrimination in employment decisions and recruitment as defined under state law.[157]

D. Non-legislative regulations and guidelines

In October 2022, the National Labor Relations Board (NLRB) issued a memo warning employers against the use of workplace surveillance and automated decision making.[158] The memo described various technologies used to monitor workers, including wearable devices, cameras, and computer tracking software. The General Counsel expressed concern that these technologies could interfere with workers' rights under the National Labour Relations Act, particularly their ability to engage in protected activities confidentially, emphasising that constant surveillance and automated management may severely limit workers' ability to exercise their rights in the workplace.

Similarly, in October 2024 the US Department of Labor published 'AI and worker well-being: principles and best practices for developer and employers.'[159] This non-binding framework aims to guide responsible AI use in the workplace, focusing on worker well-being and mitigating potential harms. The document outlines several key principles, including establishing governance and human oversight, ensuring transparency, and protecting labor rights. Additionally, the Equal Employment Opportunity Commission (EEOC) published a technical assistance document addressing the implementation of algorithmic decision-making systems in employment decisions.[160] This guidance explains how the use of such technologies by employers could potentially infringe upon the protections set forth in the Americans with Disabilities Act. The guidance offers a comprehensive overview of the potential legal pitfalls associated with these technologies, highlighting scenarios where their use might conflict with existing ADA regulations.

The latest regulatory intervention in this area is the guidance issued by the US Consumer Financial Protection Bureau (CFPB) on 24 October 2024, aimed at protecting workers from unchecked digital

154 AB-1651 Worker rights: Workplace Technology Accountability Act.(2021-2022).
155 Local Law 144 of 2021, Automated Employment Decision Tools (AEDT).
156 Illinois Artificial Intelligence Video Interview Act 2020.
157 HB3773 -The Illinois Human Rights Act.
158 'NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices' (*National Labor Relations Board*, 31 October 2022) <https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and> accessed 10 November 2024.
159 'Department of Labor Releases AI Best Practices Roadmap for Developers, Employers, Building on AI Principles for Worker Well-Being' (*DOL*, 16 October 2024) <https://www.dol.gov/newsroom/releases/osec/osec20241016> accessed 29 March 2025.
160 U.S. Equal Employment Opportunity Commission, 'The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees' <https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence>.

tracking and opaque decision-making systems.[161] While it remains uncertain whether such regulatory initiatives will continue due to the current administration's new measures, the guidance mandates that companies using third-party consumer reports — including background dossiers and surveillance-based, 'black box' AI or algorithmic scores about their workers — must follow Fair Credit Reporting Act rules. This requires employers to obtain worker consent, provide transparency about data used in adverse decisions, and allow workers to dispute inaccurate information. The guidance addresses the use of reports extending beyond traditional background checks, including apps monitoring worker conduct on their personal phones.

This evolving landscape reflects a growing recognition of the need to protect workers' data rights, particularly in light of advancing technologies such as algorithmic management.

The Australian Approach

A. Privacy and data protection legislation

Australia's approach to workers' data protection is characterised by a complex interplay of federal, State and Territory legislation, with significant differences between public and private sector workers. The principal piece of federal legislation regulating privacy and data protection in Australia is the Privacy Act 1988. The Privacy Act, initially applicable only to government agencies and extended to the private sector in 2000, sets out requirements for personal data protection, which apply to workers' personal data in the public sector. Public sector workers enjoy the same rights and protections afforded to all citizens under the Privacy Act.

However, private sector workers, who constitute the large majority of Australians,[162] are not afforded the same rights and protections. The privacy Act exempts the processing of workers' personal data by private sector employers if it is directly related to employment purposes.[163] This exemption means that 'private sector employers' are not obliged to grant workers access to their personal data, can process workers' data (including sensitive data) without consent, and are not accountable under the Privacy Act's data breach notification scheme, even if a data breach results in serious privacy harm. Private sector workers have no means of recourse under the Privacy Act if their personal data are mishandled in the workplace. Furthermore, they do not have the right to access their data under the Privacy Act to ensure fairness, prevent discrimination, and correct inaccuracies in their personal data. This makes Australia an outlier among countries with comprehensive privacy laws to specifically exclude workers' personal data from the operation of such law.[164] The Privacy Act has been subject to several inquiries since its adoption and is undergoing comprehensive reform. One of the key issues in this reform process is whether to remove the employment exemption.

The policy rationale for this exemption boils down to two related questions: (1) whether privacy protection of workers' data should be located in the Privacy Act or in another legal domain, and (2) whether workplace privacy should be regulated at the federal level or left for States and Territories.

---

161 'Consumer Financial Protection Circular 2024-06: Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions' (*Consumer Financial Protection Bureau*, 24 October 2024) <https://www.consumerfinance.gov/compliance/circulars/consumer-financial-protection-circular-2024-06-background-dossiers-and-algorithmic-scores-for-hiring-promotion-and-other-employment-decisions/> accessed 29 March 2025.

162 'For Your Information: Australian Privacy Law and Practice' (Australian Law Reform Commission (Vol 2, Report 108) 2008).

163 Privacy Act 1988 ss. 7(1)(ee) and 7B(3).

164 'For Your Information: Australian Privacy Law and Practice' (n 165).

The Australian government considers that workers' privacy is better regulated through workplace relations legislation, not privacy law.[165] In 2000, when the Privacy Act was amended to cover the private sector, the government argued that 'while (workers' personal data) is deserving of privacy protection, it is the Government's view that such protection is more properly a matter for workplace relations legislation.'[166]

The Australian government also believes that regulating workplace privacy at the federal level could create unnecessary overlap with State and Territory laws. In rejecting the recommendations by the 2000 House of Representatives Committee inquiry to remove the private-sector employee exemption, the Government stated that:

> *The regulation of employee records is an area that intersects with a number of State and Territory laws on workplace relations, minimum employment conditions, workers' compensation and occupational health and safety, some of which already include provisions protecting the privacy of employee records. The Government considers that to attempt to deal with employee records in the [Privacy Amendment (Private Sector)] Bill might result in an unacceptable level of interference with those State and Territory laws, and a confusing mosaic of obligations.*[167]

Stakeholders are divided on the policy rationale for private-sector employees' exemption from the operation of the Privacy Act. Employers and their representatives argue for retaining or strengthening the exemption, citing the existing policy rationale and suggesting that any inadequacies should be addressed in workplace relations legislation.[168] In contrast, other stakeholders including privacy advocates, privacy authorities, employee representatives and others support the removal of the exemptions. The arguments against the private-sector employees' exemption from the Privacy Act are numerous and can be summarised as follows:

1. *Lack of privacy protection for private sector employees*: Private-sector employers process vast amounts of data, including sensitive data, yet employees are left without protection. Private-sector-employees may be under economic pressure to provide personal information to their employers, effectively leaving them without choice. As highlighted above, private sector employees have no means of recourse under the Privacy Act if their personal data is mishandled in the workplace.
2. *Inadequacy of existing workplace legislation*: While the primary policy rationale for the exemption was that private-sector employees' privacy would be better regulated under workplace relations legislation, there is little privacy protection under said legislation (see sub-sec. B below).
3. *Differential treatment*: The Privacy Act protects public-sector employees but not those employed in the private sector. The Australian Government Law Reform Commission (AGLRC) points out that this lack of privacy protection for the majority of Australian employees is unjustifiable and represents a significant gap in privacy regulation. There is no sound policy for

[165] 'Government Response to the Privacy Act Review Report' (Attorney-General's Department 2023) <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report> accessed 29 March 2025; Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000.

[166] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15752. See also Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 4, [109].

[167] 'For Your Information: Australian Privacy Law and Practice (ALRC Report 108) Vol.1' (Australian Law Reform Commission 2008) <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/> accessed 29 March 2025.

[168] For instance, in their submission for the call to Review of the Privacy Act 1988, the Australian Chamber of Commerce and Industry (ACCI) and Australian Industry Group submitted that the exemption should be retained in its current form. See 'Published Responses for Privacy Act Review – Discussion Paper' (- *Attorney-General's Department*) <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent?_b_index=120> accessed 29 March 2025.

this differential treatment or for treating employees' data differently from other personal data.[169] The level of risk to individuals' privacy rights depends on the nature, scale and type of data processed rather than the size or type of the organisation handling it.

4. *Regulatory inconsistency*: Retaining the exemption would likely lead to further fragmentation of privacy regulation across States and Territories that have enacted legislation regulating workplace privacy. While the federal Privacy Act excludes private sector employees' data, some State and Territory laws provide limited protection (see below).
5. *Lack of meaningful recourse*: The employment exemption under the Privacy Act means that the Office of the Australian Information Commissioner (OAPC) cannot investigate complaints from private-sector employees regarding mishandled personal data. Consequently, the OAPC reported closing a significant number of complaints due to lack of jurisdiction (sub-sec. C below). In one instance, the OAPC reported:

> *'An employee's personal information was mishandled and stolen from the respondent's offices (the employer). The personal information was then used to commit identity fraud. The OAIC could not investigate whether the personal information had been appropriately secured by the respondent as the information was contained in an employee record.'*[170]

6. *Inconsistency with International standards*: The exemption has been an obstacle to the EU determining that Australia's privacy laws are adequate for the purpose of cross-border data flow under the GDPR. The EU has long held that this and other exemptions under the Privacy Act could prevent an adequacy finding, stating that comprehensive data protection law should apply to all data processing activities, regardless of the organisation's size or type.[171]

Due to these issues, several stakeholders have advocated for the removal of the employment exemption under the Privacy Act to ensure maximum coverage of agencies, firms, and organisations and to promote consistency. They contend that the Privacy Act is a more appropriate regulatory framework to address privacy risks than workplace relations laws, which primarily focus on working conditions such as ensuring correct wages and entitlements.[172]

The reform process of Australia's privacy landscape is ongoing. In February 2023, the Attorney-General released the final Privacy Act Review Report, recommending modifying the exemption to extend enhanced privacy protections to private sector employees while maintaining flexibility for employers. The Government initially 'agreed in-principle' with this proposal, stating that further consultation should be undertaken.[173] Despite this apparent progress, the newly introduced legislation retains the exemption, leaving private sector employees without the protections afforded to their public sector counterparts.[174] This would mean that public employees would continue to enjoy a higher level of privacy protection than the majority of Australian workers employed in private sector.

Although Australia lacks comprehensive federal legislation addressing workplace privacy, States and Territories can enact their own workplace-focused privacy laws. Under Australian law, workplace privacy law falls under industrial relations legislation, with the primary law being the Fair

169 ibid.
170 'Privacy Act Review – Discussion Paper' (Submission by the Office of the Australian Information Commissioner 2020) <https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-4-exemptions> accessed 29 March 2025.
171 For submissions by the WP29 and the Commission, see 'Published Responses for Privacy Act Review – Discussion Paper' (n 171).
172 Submission by the Office of the Australian Information Commissioner, 23 December 2021
173 'Government Response to the Privacy Act Review Report' (n 168).
174 Privacy and Other Legislation Amendment Act 2024 (NO. 128, 2024).

Work Act 2009. For instance, Section 27(2)(m) of the Fair Work Act expressly preserves the legislative capacity of States and Territories to regulate 'workplace surveillance'. However, only three jurisdictions− New South Wales (NSW), the Australian Capital Territory (ACT), and Victoria − have legislated specifically on workplace surveillance to varying degrees, applicable to both private and public entities.

The State of Victoria's *Surveillance Devices (Workplace Privacy) Act* 2006, which amends the Surveillance Devices Act 1999 to make it applicable in workplaces, provides limited physical privacy to workers. It prohibits employers from using optical, tracking and data surveillance devices in sensitive workplace areas like toilets and change rooms.[175] It also prohibits the use of optical surveillance or listening and tracking devices in certain circumstances by employers.[176] Similarly, the *NSW Workplace Surveillance Act* 2005 and ACT *Workplace Privacy Act* 2011 both require employers to give prior notice to employees for certain types of surveillance, including optical surveillance (such as CCTV, camera, and video monitoring), data surveillance such as computer monitoring of emails and websites accessed, and tracking surveillance such as GPS tracking and installing apps on mobile phones. These State and Territory laws are limited in scope and the matters they regulate.

B. Labour law and other legislative rules

While the policy rationale for the Privacy Act' exemption was that workers' privacy would be better regulated through workplace relations legislation, the Fair Work Act 2009, which is the primary federal legislation governing this area, offers only very limited privacy protections. The Fair Work Act requires employers to keep certain employee records for inspection purposes, but it does not directly address privacy rights.[177] It focuses on record keeping and compliance with workplace laws rather than protection of privacy.[178]

In fact, the Fair Work Act makes several references stating that various privacy-related issues may be regulated under the Privacy Act. Consequently, the role of the Fair Work Act versus the Privacy Act in the workplace remains uncertain, as demonstrated in the case of *Jeremy Lee v Superior Wood Pty Ltd*.[179] A 2019 Fair Work Commission decision in *Jeremy Lee v Superior Wood Pty Ltd* illustrates the regulatory uncertainty created by the Privacy Act's exemption. The Full Bench ruled that an employer's direction to an employee to submit to fingerprint scanning to record attendance violated the employee's right to withhold consent for sensitive information collection under the Privacy Act. According to this decision, the Privacy Act's exemption only applies after an employee's data have been collected; it does not apply to records that did not yet exist. This case is significant due to the rapid development of biometric data collection technologies in the workplace. As Peter Holland pointed out, it underscores the lack of legislative clarity and arbitrary nature of legal protection surrounding such data collection.[180]

Furthermore, Section 205 of the Fair Work Act requires all enterprise agreements to include a term mandating the employer consult employees' representatives about a major workplace change likely to have a significant effect on employees (such as termination, alternation of working hours,

175 *Surveillance Devices Act 1999* (as amended in 2006) s 9B.

176 The State of Victoria has launched a new inquiry into workplace surveillance with unions proposing new standalone legislation limiting surveillance against workers. See 'Submissions - Inquiry into Workplace Surveillance' (*Parliament of Victoria*) <https://www.parliament.vic.gov.au/get-involved/inquiries/inquiryintoworkplacesurveillance/submissions/> accessed 29 March 2025.

177 The basis for these provisions is to ensure records are available for inspection by workplace inspectors and authorised union officials to ensure compliance with workplace laws.

178 'Privacy Act Review Report 2022' (Australian Government Attorney General's Department).

179 *Jeremy Lee v Superior Wood Pty Ltd [2019] FWCFB 2946 (1 May 2019)*.

180 Peter Holland, 'Workplace Biometric: Major Weaknesses in Protecting Employee Privacy (Submission Privacy Act Review – Discussion Paper)' <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/view_respondent?_b_index=0&uuId=457461490> accessed 29 March 2025.

restructuring of jobs). However, it is unclear if the introduction of new surveillance technologies would constitute a major workplace change. Stakeholders have expressed concerns that current provisions within the Fair Work Act providing for consultation with workers are insufficient to ensure necessary worker engagement and voice regarding workplace surveillance and automated decision-making technologies.[181]

Lessons from other jurisdictions

This section provides an overview of workers' data protection regimes in several African countries and Latin America, with specific focus on Brazil, as well as India and China. It aims to draw useful insights from these jurisdictions and to identify existing regulatory gaps. By examining these diverse legal frameworks and recent policy developments, this section highlights both advances and shortcomings in protecting workers' data rights across emerging and advanced economies.

Privacy and data protection regulations in Africa have made significant progress in recent years, with majority of the countries now having adopted comprehensive data protection laws. At the time of this writing, over 39 African nations have implemented such legislation, while several others are in the process of consideration.[182] These laws are largely influenced by regional and international frameworks, including the African Union Convention on Cyber Security and Personal Data Protection, the GDPR and the Council of Europe's Convention 108+, incorporating fundamental data protection principles.

Building on this foundation, a common trend among African data protection laws is the inclusion of protections for data subjects against certain types of fully automated decision-making, which is particularly relevant in the employment context. Reports indicate that approximately 35 African data protection laws recognise the right not to be subject to solely automated decision-making, similar to Article 22 of the GDPR.[183] While most African data protection laws do not have explicit reference to workers' personal data or exempt workers' data processing from their scope, it is generally assumed that these general rules and principles apply to the employment context. Nevertheless, the lack of specificity in addressing the unique needs of employment relationship remains a notable gap.

This gap becomes even more apparent when considering the relationship between workplace relations legislation and data protection. Some African data protection laws refer to labour legislation, although existing labour laws typically lack modern data protection rules beyond general record-keeping requirements. For instance, South African data protection law mandates that employers process personal data concerning worker's criminal behaviour or biometric data in accordance with labour legislation.[184] However, the absence of comprehensive workplace-focused data protection legislation across the continent means that many employment-specific issues are not adequately addressed. Notably, no African country has yet adopted or considered workplace-focused data protection legislation, leaving workers vulnerable to evolving technological practices.

Moving to enforcement and institutional arrangements, most African data protection laws have established regulatory bodies for enforcement, though the independence of some authorities

181 'Published Responses for Privacy Act Review – Discussion Paper' (n 171).

182 Dorcas Tsebee and Ridwan Oloyede, 'DPAs and AI Regulation in Africa' <https://iapp.org/news/a/dpas-and-ai-regulation-in-africa> accessed 14 November 2024; 'Which African Countries Have a Data Protection Law?' (*Data Protection Africa | ALT Advisory*, 14 November 2023) <https://dataprotection.africa/which-african-countries-have-a-data-protection-law/> accessed 14 November 2024; Dorcas Tsebee and Ridwan Oloyede, 'Roundup on Data Protection in Africa 2023' (Tech Hive 2023).

183 Tsebee and Oloyede, 'DPAs and AI Regulation in Africa' (n 185).

184 Protection of Personal Data Act 2023 s 33.

remains uncertain.[185] Despite this, some of these authorities have been proactive in taking enforcement measures and issuing workplace-specific regulations and guidance. For example, Senegal's Personal Data Protection Commission (PDPC) rejected a company's application to use facial recognition technology for monitoring worker attendance,[186] and subsequently issued guidance on using biometric technologies in the workplace.[187] Similarly, the Moroccan Data Protection Authority has taken administrative measures, including a moratorium on the use of facial recognition technology,[188] and co-sponsoring a Resolution on AI and employment at Global Privacy Assembly.[189]

The challenges posed by emerging technologies are further compounded by the lack of AI-related regulation specifically targeting the employment context. While there are several AI-related initiatives in Africa, they generally focus on regulating AI broadly rather than specifically addressing algorithmic management and automated decision-making in the employment context. The absence of employment-specific data protection and labour legislation in some African countries has contributed to the continued exploitation of workers by big tech companies outsourcing their AI work to countries with less or no regulatory intervention.[190] In conclusion, while Africa has made significant strides in data protection legislation, there remains a need for more targeted regulation addressing the unique challenges posed by emerging technologies in the workplace. Without such measures, the continent risks falling behind in safeguarding workers' data rights and ensuring fair labour practices in the digital age.

Data protection frameworks in Latin America largely mirror the regulatory approaches seen in Africa, with most jurisdictions lacking explicit statutory provisions tailored to the workplace data processing. Instead, general data protection rules−often modelled after the EU's GDPR− apply to employment relationships by default, but without detailed guidance on employment-specific scenarios. Brazil's General Data Protection Law (Lei Geral de Protecao de Dados, LGPD), effective since 2020, exemplifies this trend. The LGPD establishes a comprehensive regime for personal data processing across both public and private sectors articulating broad principles, individual rights and organisational obligations. However, it does not delineate specific rules for processing workers' data.[191] As a result, workplace data practices in Brazil are shaped by the LGPD's general provisions in conjunction with evolving labour jurisprudence.[192] Reports shows that judicial trends in Brazil increasingly reflect the LGPD's influence, with courts adjudicating disputes over the boundaries of permissible workplace data processing.[193] For instance, employers have sought to use geolocation data from workers' mobile devices to verify compliance with working hours.

185 'How Independent Are African Data Protection Authorities?' (*Data Protection Africa | ALT Advisory*, 28 June 2023) <https://dataprotection.africa/standing-alone-the-independence-of-african-data-protection-authorities/> accessed 14 November 2024.

186 'Quarterly Notice N°01-2023 of the Senegal Personal Data Protection Commission (CDP)' <https://www.cdp.sn/content/avis-trimestriel-n%C2%B001-2023-de-la-commission-de-protection-des-donnees-personnelles-du-0> accessed 14 November 2024.

187 'Senegal: CDP Releases Guidance on Processing of Biometric Data in the Workplace' (*DataGuidance*) <https://www.dataguidance.com/news/senegal-cdp-releases-guidance-processing-biometric-data> accessed 14 November 2024.

188 Tsebee and Oloyede, 'DPAs and AI Regulation in Africa' (n 185); Dorcas Tsebee and Ridwan Oloyede, 'State of AI Regulation in Africa: Trends and Developments' (Tech Hive 2024).

189 '45th Closed Session of the Global Privacy Assembly October 2023 Resolution on Artificial Intelligence and Employment'.

190 Adrienne Williams, Milagros Miceli and Timnit Gebru, 'The Exploited Labor Behind Artificial Intelligence' (*NOEMA*, 13 October 2022) <https://www.noemamag.com/the-exploited-labor-behind-artificial-intelligence> accessed 14 November 2024; Chloe Xiang, 'OpenAI Used Kenyan Workers Making $2 an Hour to Filter Traumatic Content from ChatGPT' (*VICE*, 18 January 2023) <https://www.vice.com/en/article/openai-used-kenyan-workers-making-dollar2-an-hour-to-filter-traumatic-content-from-chatgpt/> accessed 14 November 2024; 'Open Letter to President Biden from Tech Workers in Kenya' (*Foxglove*) <https://www.foxglove.org.uk/open-letter-to-president-biden-from-tech-workers-in-kenya/> accessed 14 November 2024.

191 Antonio Rodrigues de Freitas Júnior, Letícia Ferrão Zapolla and Paulo Fernando Nogueira Cunha, 'The Regulation of Artificial Intelligence in Brazil' (2024) 77 ILR Review 869.

192 'Privacy (and Technology) in Workplaces: A Brief Overview of Brazilian Law and Practices to Ensure Employee Privacy' <https://www.dentons.com/en/insights/articles/2023/february/24/a-brief-overview-of-brazilian-law-and-practices-to-ensure-employee-privacy> accessed 9 May 2025.

193 Renata Neeser, 'Brazil Data Protection Law – Litigation in the Context of Employment' (26 February 2024) <https://www.littler.com/news-analysis/asap/brazil-data-protection-law-litigation-context-employment> accessed 9 May 2025.

Some courts have denied such request, citing the need to protect workers' privacy, thereby underscoring the tension between workplace monitoring and fundamental rights. Other emerging issues under the LGPD include background checks, the use of publicly sourced data, discrimination, and the deployment of algorithmic management systems.

Regarding algorithmic management, Brazil's AI Bill (Bill No. 2.338/2023), recently approved by the Senate, establishes a comprehensive, risk-based framework for AI development, use and governance, closely paralleling the EU's AI Act.[194] It imposes stricter requirements on high-risk systems, particularly those impacting fundamental rights, or employment decisions.

It requires that AI providers must conduct risk assessments and implement robust governance structures to ensure compliance and security. Notably, the bill introduces mandatory human oversight for automated workplace decisions, aiming to prevent fully automated dismissals and requiring perioding impact assessments to safeguard worker-well-being. For example, Article 14 of the bill sets out an extensive list of AI systems considered 'high-risk' including AI systems used for recruitment, screening, evaluation of candidates, decision-making about promotions or terminations of employment contracts, performance evaluations, or behavioral assessments affecting employment, worker management, or self-employment access.[195] While some labour protections, such as restrictions on workers' participation in impact assessments, were reportedly diluted in the legislative process,[196] key safeguards remain, including specific mandates for sectoral authorities, in coordination with the Ministry of labour, to develop guidelines mitigating negative impacts on employment and maximizing positive outcomes, including workplace safety and continuous professional development. The legislation articulates extensive list of principles and values such as non-discrimination, privacy, the right to contest AI-driven decisions.[197]

In India, the Digital Personal Data Protection Act (DPDP Act) 2023 provides that data fiduciaries (controllers) may lawfully process personal data only with the consent of the data principal (data subject) or for certain specified 'legitimate uses'[198] Processing of personal data for 'employment purposes' is listed as 'legitimate use' under Sec. 7(i). This provision makes a significant shift in India's approach to workers' data protection by permitting employers to process workers' data without explicit consent under the 'legitimate use' ground and thus creates critical ambiguities and risks. It risks normalising non-consensual data practices in the workplace where workers may lack meaningful avenues to challenge misuse. The Act does not define 'employment purposes', leaving unclear whether pre-employment activities such as background checks and interviews, or intrusive monitoring practices (e.g. productivity tracking) fall under this exemption. This ambiguity creates uncertainty for both workers and employers. For instance, a former employer may lack a clear legal basis to share an ex-worker's data for background checks without consent after the employment termination. The Act's 'legitimate use' ground for employment purposes applies only during active employment, not-post-termination. Since the exemption no longer covers ex-workers, the former employer cannot rely on it to process or disclose data unless the worker's original employment contract explicitly included consent for future background checks. Absent such prior contractual consent, the employer risks non-compliance, as the APDP Act mandates explicit consent for third-party data sharing.[199]

---

194 Jorge Vinícius Corrêa Portela, 'Regulatory framework for artificial intelligence passes in Brazil's Senate' (*Mattos Filho*, 11 December 2024) <https://www.mattosfilho.com.br/en/unico/framework-artificial-intelligence-senate/> accessed 9 May 2025.

195 Article 14 (III), Bill No. 2338/2023 (Translated at www.deepl.com) .

196 Rafael AF Zanatta and Mariana Rielli, 'The Artificial Intelligence Legislation in Brazil: Technical Analysis of the Text to Be Voted on in the Federal Senate Plenary' (*Data Privacy Brasil Research*, 10 December 2024) <https://www.dataprivacybr.org/en/the-artificial-intelligence-legislation-in-brazil-technical-analysis-of-the-text-to-be-voted-on-in-the-federal-senate-plenary/> accessed 10 May 2025.

197 Articles 2 and 3, Bill No.2338/202.

198 Digital Personal Data Protection Act 2023 s 4.

199 Expert Response India.

Workers' data protection in China is governed by patchwork of legislation, including the Personal Information Protection Law (PIPL), Labour Contract Law, and employment-related provisions. Article 13 of the PIPL allows employers to process workers' data without consent when necessary for contract performance or human resources management under lawful labour rules and collective agreements. However, sensitive data processing or third-party disclosure require explicit consent, ensuring workers retain control over their personal information. The Labour Contract Law obliges employers to disclose relevant job-related information during recruitment and permits inquiries into basic details directly related to employment contracts, thereby promoting transparency. Additionally, employers are obliged to maintain the confidentiality of workers' data and must obtain written consent before disclosure workers' data to a third-party.

▶ 4 Regulatory gaps, challenges, and uncertainties

There is no uniform and consistent approach to workplace data protection; approaches differ markedly across jurisdictions and legal frameworks. However, three broad categories of data protection laws can be identified globally based on the extent to which they apply to the workplace.[200]

The first category covers data protection laws that include specific provisions exclusively dealing with workers' data protection. While the early data protection regimes were silent on this matter, several modern data protection laws such as the GDPR and several EU Member States laws, incorporate specific provisions tailored to the employment context. The second category includes data protection laws that are implicitly applicable to the workplace due to their general principles and technology or context neutral regulatory approaches. Most data protection laws in Africa, Latin America and Asia fall into this category. The ILO's recent Policy Brief on Improving Workers' Data Rights indicates that most data protection regulation in the world belongs in the second category.[201] The third category includes data protection laws that explicitly exclude workers' data from their scope of application. The Australian Privacy Act and most data protection regulations in the US belong to this category.

As discussed in the preceding sections, data protection laws are not the only legal frameworks dealing with workers' data rights. These laws are often complemented by other sectoral laws addressing specific practices and technologies, and emerging digital regulations such AI-specific laws. While these legislations offer additional layer protection for workers, they also add layers of complexities and uncertainties.

One of the most interesting observations is that, despite the general agreement across jurisdictions on the need for employment-specific data protection regulations, such specific rules rarely exist. As aptly summarised by Einat Albin, 'it seems puzzling that most countries do not have specific rules for data protection in the realm of employment, relying instead on general data protection laws... As a result, norms that were neither conceived with the world of labour in mind nor conform to the framework of labour law are brought to bear on the realm of employment'.[202]

The analysis of workers' data protection frameworks across jurisdictions also reveals significant regulatory gaps, uncertainties, and systemic challenges. This section examines these issues across six interrelated key dimensions to provide a comprehensive understanding of the current landscape.

Inadequacy of general data protection frameworks

The analysis clearly demonstrates that omnibus data protection frameworks, while providing baseline protections, are fundamentally inadequate to address the distinct challenges of employment relations and the novel challenges posed by advanced surveillance and decision-making technologies. This is particularly true in jurisdictions where general data protection laws' applicability to the workplace is only implicitly recognised. The gap exists even in jurisdictions where

200 See also 'Improving Workers' Data Rights' (ILO brief 1 2022) <https://www.ilo.org/publications/improving-workers-data-rights> accessed 29 March 2025.
201 ibid.
202 Albin (n 106).

data protection laws include specific provisions dealing with workers' data protection, though to a different extent.

For instance, despite the GDPR's comprehensive approach to data protection, its generalised framework fails to account for the power imbalances, collective interests, and unique requirements of workplace data processing. This inadequacy has been recognised since the early days of data protection legislation and the GDPR itself. The GDPR assumed that employment-related data processing would be regulated by separate rules. When recently asked if there was anything he regretted about the GDPR text in retrospect, Jan Philipp Albrecht, the rapporteur for the GDPR at the time, identified 'employment' as an area not fully regulated by the GDPR.[203]

Despite recognising the need for workplace-specific data protection rules, legislative efforts to introduce such laws have repeatedly failed. The overlapping constitutional powers to legislate on industrial relations, coupled with diverse traditions among Member States regarding employment relations, makes it complex for the EU to harmonise workers' data protection effectively. While the GDPR acknowledges the special nature of personal data processing in employment contexts, it simply delegates the responsibility to Member States through Article 88(1). Member States, in their part, failed to fully take this opportunity, leaving Member State data protection laws in the employment context as patchy, inadequate, and inconsistent. The CJEU's ruling in Case C-34/21 highlighted above further confirms this finding, as it invalidates key aspects of German data protection legislation dealing with the employment context, prompting the introduction of a new legislative proposal, the Employee Data Protection Act 2024.[204] This decision underscores that merely extending general data protection principles and requirements to the employment context without accounting for the specific needs of labour relations is inadequate.

Treating workers as consumers

In its Opinion 8/2001, the European Data Protection Working Party (WP29) declared that 'workers are data subjects'.[205] 'Any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of (data protection legislation)', the WP29 continued. This means that, as a general rule, workers enjoy the rights and protections offered by omnibus data protection legislation. The problem with this approach is that it conceives workers as 'consumers' (data subjects), failing to account for the stark difference between consumer-data controller and employment relations, including the power dynamics and subordination. As Albin notes, data protection law's 'conception of the data subject contradicts labour law's specific conception of the employee'.[206] Furthermore, workplace data protection issues are 'not just consumer issues; they are also labour rights issues'.[207] As discussed in the preceding sections, the impact of workplace monitoring and decision-making technologies cannot be framed in terms of privacy and data protection alone, and hence 'regulating data collection and use in the workplace is now more a matter of regulating working conditions than data protection'.[208]

---

203 European Data Protection Supervisor, *Two decades of personal data protection, what next? – EDPS 20th anniversary* (Publications Office of the European Union, 2024) https://data.europa.eu/doi/10.2804/652641

204 Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes 2024; 'Germany Draft for Employee Data Act Issued' (n 112).

205 WP 48.

206 Albin (n 106) 14.

207 Phela Townsend, 'Data Privacy Is Not Just a Consumer Issue: It's Also a Labor Rights Issue' (*Next100*, 14 May 2020) <https://thenext100.org/data-privacy-is-not-just-a-consumer-issue-its-also-a-labor-rights-issue/> accessed 23 March 2025.

208 Dan Calacci and Jake Stein, 'From Access to Understanding: Collective Data Governance for Workers' (2023) 14 European Labour Law Journal 253.

Therefore, a fundamental challenge in existing workers' data protection lies in the application of consumer-oriented, individualistic privacy and data protection frameworks to employment contexts. For instance, the GDPR establishes general data protection principles and legal bases that apply uniformly across contexts. However, these provisions may operate differently in employment settings due to inherent power imbalances. For instance, while consent is a prominent legal basis under the GDPR, its validity in employment contexts is questionable given the economic pressure workers face. Recognising this issue, proposals during the GDPR's development included provisions to exclude consent as a valid legal basis for processing workers' personal data, though these provisions were ultimately not incorporated.

By applying consumer-oriented frameworks to employment contexts without accounting for their unique characteristics, regulators fail to address the specific vulnerabilities workers face regarding their data rights. In other words, the legislation that protects us as consumers falls short in protecting us as workers.[209]

Complex overlap with other legal fields

Does the protection of workers' data fall under data protection legislation or labour law, where the employment relations are governed? The protection of workers' data sits at the intersection of multiple legal domains, including data protection law, labour law, OSH, emerging digital regulations (e.g., AI regulations) and other sector-specific laws offering indirect or incidental protections. This overlap can result in regulatory uncertainty, contradictions, and enforcement challenges. While recognising these complex webs of relevant legal domains, this section focuses on the interaction between labour law and data protection and the resulting challenges and opportunities in protecting workers' data rights.

In some jurisdictions, for instance Australia, the regulation of workers' privacy and data protection rights falls under labour law rather than data protection legislation. As discussed above (Section 4.2.3), one of the policy rationales for the exemption of private-sector workers' data from the scope of the Privacy Act is that workers' privacy is considered better regulated through workplace relations legislation rather than privacy law. However, privacy advocates, privacy authorities, and workers' representatives in Australia argue that the Privacy Act is a more appropriate regulatory framework to address privacy risks than workplace relations laws, which primarily focus on working conditions such as ensuring correct wages and entitlements.[210]

The situation slightly differs in Europe. In its Opinion 8/2001, the WP29 emphasised that the protection of workers' data falls primarily within the scope of data protection legislation rather than labour law while acknowledging 'the necessary interaction between the two'. The Working Party argued that 'data protection law does not operate in isolation from labour law and practice, and labour law and practice does not operate in isolation from data protection law'. While the extent and precise nature of this interaction varies between Member States, the Working Party noted:

1. The increasing use of advanced technologies in the workplace amplifies this interaction because employment practices rely more and more on personal data processing subject to general data protection principles;

209 Townsend (n 210).
210 See 'Submissions - Inquiry into Workplace Surveillance' (n 179).

2. Not all problems arising in employment contexts involving personal data processing are exclusively related to data protection;
3. This interaction is necessary and valuable, assisting in developing solutions that properly protect workers' interests.

Despite divided opinions among stakeholders regarding how labour and data protection laws should interact, there is a clear consensus that their overlap is unavoidable. Workers' data protection falls under both labour law and data protection law, while other fields of law also offer direct or incidental protections. This cross-cutting nature has become increasingly pronounced with new technologies such as algorithmic management, which blurs traditional legal boundaries and creates a complex regulatory landscape.

The intersection creates valuable opportunities as different areas of law can complement each other to offer workers comprehensive protections. As the WP29 explicitly acknowledged, integrating labour law and data protection legislation is 'necessary and valuable' for developing solutions that properly protect workers' interests. Effective protection of workers' data rights thus requires reimagining data governance across disciplines by combining legal frameworks and coordinating regulatory bodies. This interdisciplinary approach is evident in cases like Uber Amsterdam, where platform workers utilised the GDPR's data access rights to strengthen their collective bargaining position. This approach can also shed light on the inner workings of the algorithmic management tools with significant impact on working conditions.

However, this overlap also presents significant challenges due to diverging legal traditions, concepts and objectives. Labour law traditionally favours collective solutions over individualistic approaches by recognising workers' unequal bargaining power and emphasising non-waivable minimum standard across workplaces. In contrast, data protection law often takes a more individualistic approach.

The overlap between these legal domains blurs established categories, potentially causing workers' data rights to fall through the cracks. Data protection law may be too generic to address specific employment issues, while labour law may be too specific to comprehensively cover all data protection concerns in the workplace. Furthermore, enforcement confusion arises when authorities lack clear jurisdiction or expertise to address hybrid issues effectively. Achieving coherence across overlapping legal instruments remains a significant challenge, highlighting the need for sector-specific, employment-focused data protection regulations to bridge gaps and provide comprehensive protections for workers.

Structural legal deficits

The challenges created by the intersection of labour law and existing data protection regulations ultimately result in what Einat Albin calls 'structural legal deficit'.[211] Albin identifies a three-tier structural deficit undermining workers' data rights:

1. Labour law frameworks treat workplace technologies as employer-owned commodities, granting broad prerogatives to deploy them with minimal legal constraints —legitimising extensive data collection and analysis as part of employer authority while amplifying power imbalances.

[211] Albin (n 106).

2. Data protection laws such as the GDPR inadequately address labour-specific dynamics by treating workers as consumers or data subjects without integrating labour law principles effectively.
3. Consequently, workplace-related data governance remains detached from labour law's collective mechanisms such as collective bargaining.

Albin argues that this threefold deficit– rooted in employer-centric technology adoption, individualistic approaches in data protection laws, and exclusion of collective tools– creates systemic vulnerabilities for workers.

Workplace exemptions

Workplace exemptions represent one of the most significant regulatory gaps across jurisdictions, particularly in countries like the US and Australia. These exemptions create substantial vulnerability for workers by excluding employment-related data from protections applicable elsewhere. In Australia, for instance, the regulatory distinction between public and private-sector workers creates an inequitable system where government workers receive protection under the Privacy Act, while the private sector workers are explicitly exempted. This division has been maintained despite several reform attempts, perpetuating a significant gap for most Australian workers. Such exemptions perpetuate a two-tiered system where public sector workers enjoy greater rights than their private sector counterparts. Excluding workers' privacy rights from broader privacy and data protection laws without ensuring equivalent protections in workplace relations rules demonstrates a prioritisation of commercial interests over worker rights.

Fragmented regulatory frameworks and enforcement challenges

Workers' data protection also faces significant challenges due to fragmented, inconsistent, and complex regulatory frameworks across jurisdictions, compounded by enforcement gaps and overlapping mandates. This systemic inadequacy undermines legal certainty and comprehensive protections as workplace technologies evolve.

The EU's approach combines the GDPR, labour laws, industrial relations, emerging digital regulations (e.g. AI Act, Platform Work Directive) and other sector-specific laws offering indirect protections, creating a fragmented system with divergent substantive safeguards. It remains uncertain how the GDPR, AI Act, and the Platform Work Directive interact with each other as well as with national rules. Furthermore, Article 88(1) of the GDPR could inadvertently foster legal inconsistency across the EU unless strictly applied under Article 88(2) based on the criteria articulated by the CJEU (see Section 4.2.1).

The US and Australia represent the most patchy regulatory landscape characterised by a complex web of fragmented and inconsistent federal and state legislation. The US lacks a federal privacy law, relying instead on various sector-specific regulations and state laws that frequently exclude workplace data. Much of the workplace privacy protection in the US is derived not from data protection legislation, but from the influence of other sectoral laws. Australia's approach to workers' data protection is characterised by a complex interplay of federal, State and Territory legislation, with significant differences between public and private sector workers.

The piecemeal approach to workers' data protection exhibited across jurisdictions is further compounded by the environment of multiple regulatory authorities with potentially overlapping mandates and enforcement gaps. In the EU, data protection authorities (DPAs), which are responsible for enforcing workplace data protection rules, lack labour law expertise and rarely

prioritise workplace issue— only 1 of 11 DPAs studied included workers' data in their 2023 strategic plans. On the other hand, labour organisations and collectives do not prioritise data protection and data governance as they mostly consider these issues not to be workplace issues but instead those of individual privacy.[212] While harms from workplace technologies often require intersectional enforcement across equality, labour, and data protection laws, siloed agencies struggle to coordinate.

Similarly, the US has multiple regulatory agencies with overlapping jurisdictions and varying degrees of rulemaking and enforcement powers. At the federal level, agencies such as the Federal Trade Commission (FTC), Federal Communications Commission (FCC), National Labor Relations Board (NLRB), Consumer Financial Protection Bureau (CFPB), and Department of Health and Human Services (HHS) all play roles in enforcing different aspects of data protection and privacy laws. The enforcement powers of these regulators depend on the specific statutes under review as well as regulations, other instruments, and enforcement priorities, leading to a patchwork of rules that can be difficult to navigate and enforce consistently. At the state level, the landscape is equally varied. California has taken a pioneering step by establishing the California Privacy Protection Agency (CPPA), the first dedicated privacy regulator in the US. This move represents a significant shift towards more robust and specialised privacy enforcement. However, other states continue to rely on their Attorneys General and other agencies to conduct rulemaking or enforcement actions related to violations of their respective data protection and privacy laws. Moreover, their regulations and enforcement strategies change between administrations making it even more complex and fragmentary.

Australia's regulatory framework creates particular challenges through the division between private and public sector employee protections and the overlapping jurisdictions of regulatory authorities. There is a disagreement among Australian stakeholders on whether workplace privacy should be regulated by privacy law or workplace relations laws. Although the Fair Work Act 2009 provides very little protection, jurisdiction for private sector employee privacy matters is conferred on the Fair Work Ombudsman rather than the OAIC.[213] The Privacy Act's exemption, combined with this regulatory uncertainty, creates confusion for employees about which authority to approach and which laws apply to their situations. The fact that privacy protections for employees falls under workplace relations laws constrains the role of the OAIC in relation to privacy complaints, enforcement of privacy obligations and development of privacy codes in the employment context. This uncertainty could lead to the Fair Work Ombudsman and the OAIC taking opposing views in relation to the same privacy complaint. It may also create confusion for employees about which regulator to complain to or which law applies to their matter, illustrated by the significant number of complaints the OAIC receives concerning private-sector employees' privacy. The OAIC often notes its lack of statutory power to investigate complaints it receives concerning workplace privacy of private-sector employees: 'The OAIC received a complaint that a former employer allegedly disclosed that the complainant had been suspended from their job through an autoreply email that was connected to their work address. The OAIC could not investigate this matter due to the employee records exemption.'[214]

In conclusion, the protection of workers' data rights in the jurisdictions examined remains inadequate, patchy, inconsistent, complex, and multi-layered, making it difficult to navigate.

---

212 Justin Nogarede, Michael 'Six' Silberman and Joanna Bronowicka, 'Improving Workplace Data Protection: Achieving Workplace GDPR Compliance, Clarifying National Workplace Data Protection Rules, and Enhancing Worker Data Protection through Social Dialogue' (Friedrich-Ebert-Stiftung 2024).

213 'Privacy Act Review – Discussion Paper' (n 173).

214 ibid.

5 The future of workers' data rights: towards a balanced regulatory approach

The regulatory frameworks for workers' data protection across the jurisdictions reveal significant gaps and challenges that undermine effective protection. Structural barriers, workplace exemptions, inappropriate application of consumer-oriented frameworks to employment contexts, overlapping legal fields, and fragmented regulatory systems all contribute to a landscape where workers' data rights remain inadequately protected.

These issues are particularly concerning given the rapid advancement of workplace surveillance technologies and algorithmic management systems that pose new and evolving risks to workers' privacy, dignity and autonomy.

Future regulatory approaches must address these fundamental challenges to ensure that workers receive appropriate and consistent data protection. This will require greater harmonisation of standards, removal of workplace exemptions, clear delineation of regulatory authorities' responsibilities, and recognition of the unique power imbalance inherent in employment relations that is further reinforced by advanced technologies and management systems.

The necessity for specialised data protection legislation

While other areas of law remain relevant, data protection law holds a central role in regulating workplace technologies due to the vast amounts of data underpinning these systems. Properly designed and enforced workers' data protection law could serve as a powerful tool to mitigate risks posed by algorithmic management, digital monitoring, and other emerging technologies. Moreover, the rapid digitalisation of workplaces and adoption of advanced surveillance and decision-making technologies expose critical gaps in omnibus data protection frameworks like the GDPR, underscoring the urgent need for specialised rules tailored to employment relations.

While omnibus regulations offer baseline protections, they fall short in addressing the unique complexities of labour relations and the novel risks associated with digitalisation in the workplace. Existing data protection laws often lack provisions specific to workplace contexts or fail to address the nuanced requirements of labour relations. Even laws with explicit workplace-specific provisions remain insufficient to tackle the complexities inherent in employment relationships. Regulating workplace data is inherently intertwined with regulating labour conditions; as scholars have emphasised, data collection and use in employment settings is more about working conditions than traditional data protection concerns.[215] Despite this reality, current regulations are rarely designed with labour relations in mind, reflecting the tendency to treat workers as consumers.[216]

This inadequacy highlights the urgent need for tailored rules that prioritize workers' data rights and reflect the realities of modern employment. These rules should address the realities of employment, including workers' unequal bargaining power, and emphasise non-waivable minimum

[215] Calacci and Stein (n 211).
[216] Albin (n 106).

standards across workplaces. Importantly, such regulations must be informed by labour law principles rather than consumer-oriented approaches, ensuring that protections are meaningful within the employment contexts.[217]

The imperative of workplace-specific data protection rules informed by labour law principles is recognised by the ILO's Code of Practice. Acknowledging the fundamental nature of workers' rights and the inherent power dynamics of employment relations, the Code of Practice prescribes that workers' data rights are non-waivable[218]– a stance that contrasts with modern consumer-oriented data protection regimes.

In this regard, it is promising to observe a renewed focus on workers' data rights and emerging pathways for improvement. For instance, Germany's draft Employee Data Protection Act 2024 aims to address gaps in workplace-specific data protection, responding to legal uncertainties highlighted by recent court rulings. Similarly, the EU's Platform Work Directive (PWD) establishes a comprehensive framework for regulating workplace digital monitoring and algorithmic management in platform work. While its scope is limited to platform workers, the PWD offers a blueprint for future legislative advancements in this area. Together, these initiatives signal a growing recognition of the need for robust legal frameworks tailored to protect workers' rights in an increasingly digitalised world.

In terms of substantive content, it is recommended that workplace-specific regulations address the key elements described below.

Clarifying the personal scope of workplace data protection rules

Workplace data protection rules must adopt a comprehensive approach, encompassing the entire employment relationship and safeguarding all workers, regardless of their legal status or nature of their employer organisation. Digital monitoring in the workplace often functions as a continuous feedback loop– beginning pre-hire phase, permeating daily work activities, and frequently extending into post-employment. Consequently, workplace data protection rules should apply uniformly to job applicants, employees, independent contractors, and ex-employees to ensure consistent protections throughout all stages of the employment relationship.

The Platform Work Directive, which seeks to regulate algorithmic management on digital labour platforms, notably excludes traditional employees from its personal scope. This exclusion creates an incoherent regulatory environment that places many workers in legal uncertainty.[219] Safeguarding human dignity, legitimate interests and fundamental rights of workers should not depend on the legal nature of the employment relationship. Unless explicitly stated otherwise (such as in cases where collective rights are exclusively reserved to trade unions) and without prejudice to national peculiarities, workplace data rules should apply to all types of workers irrespective of their employment status.

Similarly, adopting a two-tiered framework that differentiates between public and private-sector workers' data risks fragmented protections that fail to uphold consistent standards across workplaces. Workplace data protection rules should avoid such differential treatment to ensure fairness and uniformity in safeguarding workers' data rights across all sectors and employment contexts.

---

217 Recommendation No. R (89) 2.

218 ILO Code of practice on the protection of workers' personal data 1997 para 5.13.

219 Aída Ponce Del Castillo and Diego Naranjo, 'Regulating Algorithmic Management: An Assessment of the EC's Draft Directive on Improving Working Conditions in Platform Work' (ETUI Policy Brief 2022).

Establishing fair balance between workers' and employers' interests

The most challenging aspect of workplace data protection is striking a fair balance between employers' legitimate interests and workers' specific rights to dignity, privacy, and other fundamental rights. The question of proportionality arises specifically when workers' data processing goes beyond what is strictly required within the contractual employment relationship. Any processing of workers' data that is not strictly necessary for the performance of the contract may be carried out only after a balancing of interests. This includes interpreting the limits of an employer's 'legitimate interest', which is often used as a primary legal basis to deploy automated monitoring and decision-making technologies in the workplace.

Unfortunately, existing laws do not offer clear frameworks for conducting such a balancing exercise. What constitutes legitimate interest remains uncertain, context-dependent, and prone to abuse. It changes over time, in different contexts, and across business models. Employers can easily argue that any form of monitoring and surveillance in the workplace is proportionate and necessary for the business interests and purposes they define themselves, including improving productivity, efficiency, and innovation. Employers are expected to conduct this balancing exercise, irrespective of the type of data practice, technology used, or the legal basis for processing. However, it should not be solely the responsibility of employers to weigh these interests. While it is not feasible for legislatures to address every possible data processing activity in the employment context, they can establish clear principles and requirements to guide employers. As the German Advisory Council on Employee Data Protection aptly pointed out, there must be binding and reliable rules enabling employers and workers to assess, with legal certainty, which decisions and measures are permissible, and which are not.[220] In other words, new workers' data protection legislation should specify the criteria and requirements for the proportionality test. It should also delineate the contexts, purposes, practices, and processing activities that are off-limits, including the continuous or permanent monitoring of workers' behaviour.[221] Lawmakers should also consider the circumstances and processing operations in which 'legitimate interest' cannot be invoked as a valid legal ground.

Collective governance of workplace data practices

The case for collective governance of workplace data rights emerges from the need to address systemic power imbalances and collective risks in modern employment. While individual rights under existing data protection regimes like the GDPR provide crucial protections, they fail to counterbalance the inherently unequal dynamics of employment relationships, which are amplified by new automated decision-making and pervasive surveillance systems. This necessitates shifting from an individual consent model to mechanisms empowering workers' representatives to negotiate data practices, participate in technology design, and audit systems. This means that the deployment of workplace digital monitoring and decision-making technologies should not be left to the prerogatives of the employer.

The GDPR's article 88 implicitly supports this approach by encouraging Member States to develop workplace-specific data protections rules through social dialogue, prioritising human dignity and workers' fundamental rights. Like other labour rights such as wages and working hours, these

220 'Interdisciplinary Council on Employee Data Protection' <https://www.denkfabrik-bmas.de/en/topics/employee-data-protection/interdisciplinary-council-on-employee-data-protection> accessed 29 July 2023.

221 For details on this, see Adams-Prassl and others (n 4), Policy options 1-2.

technologies and practices should be negotiated through social dialogue. Recent legislative developments, such as Spain's Royal Decree Law 9/2021 and the EU Platform Work Directive, reinforce this trajectory by mandating transparency about algorithmic parameters to worker representatives and mandating their involvement in crucial decisions such as data protection impact assessments. A robust collective data governance framework would institutionalise rights like prior consultation and participation on the adoption of workplace technologies, participation in impact assessments, and collective access to data informing workplace decisions.

Critically, collective governance counters the limitations of consumer-centric data protection laws by integrating labour rights like co-determination, information, consultation, and collective bargaining into workplace data protection regimes. This approach aligns with evidence showing that worker participation in technology implementation reduces exploitation risks while fostering trust. For instance, requiring employer negotiated agreements on surveillance tools prevents unilateral impositions of intrusive monitoring systems. By embedding these principles, policymakers can ensure workplace data rules reflect the collective nature of labour relations, balancing technological innovation with protections against algorithmic arbitrariness and dehumanising managerial practices. Future regulatory frameworks should strengthen existing representation mechanisms and establish new mechanisms to ensure that workers have genuine agency in decisions regarding their personal data.

Emergence of specialized regulation for algorithmic management

This research reveals a significant regulatory shift toward specialised frameworks for addressing algorithmic management in the workplace, which has now transcended its origins in the platform economy and is infiltrating conventional workplaces.[222] These emerging frameworks suggest a regulatory trajectory moving away from one-size-fits-all approaches toward sector-specific protections that acknowledge the unique challenges of automated decision-making in employment settings. Future regulatory developments should continue in this direction, expanding beyond platform work and addressing algorithmic management across all employment contexts while establishing bright-line rules and reinforcing transparency requirements, and meaningful involvement of worker representatives in all stages of algorithmic management systems, from procurement, configuration, and deployment to evolution, auditing and impact assessment.

The need for cross-regulatory cooperation

The imperative for cross-regulatory cooperation in workplace data protection stems from the multidimensional risks posed by advanced monitoring and decision-making technologies, which straddle multiple legal domains and regulatory jurisdictions. These technologies inherently intersect with labour rights, equality frameworks, and data protection, creating complex challenges where siloed enforcement mechanisms risk legal fragmentation and inconsistent oversight. While DPAs focus on privacy/data protection issues, labour inspectors address working conditions, and equality bodies combat discrimination, with the result that their siloed mandates could fail to address the compounded harms arising from advanced monitoring and decision-making systems.

[222] Uma Rani, Annarosa Pesole and Ignacio González Vázquez, 'Algorithmic Management Practices in Regular Workplaces: Case Studies in Logistics and Healthcare' (Luxembourg: Publications Office of the European Union, 2024).

This regulatory fragmentation underscores the need for integrated governance models that harmonise enforcement across disciplines. Emerging frameworks like the EU Platform Work Directive exemplify progress by mandating collaboration between DPAs and labour authorities and requiring information-sharing about algorithmic systems impacting platform workers.[223] Broader initiatives such as the EU Digital clearinghouse,[224] the UK's Digital Regulation Cooperation Forum (DRCF),[225] and the Dutch Digital Regulation Cooperation Platform (STD)[226] demonstrate growing recognition of this interdependence. However, these models require adapting to employment contexts through institutional reforms that embed permanent coordination mechanisms between relevant authorities, such as data protection, labour and equality bodies. Effective implementation demands joint investigations, unified guidance on overlapping legal obligations, and shared expertise in auditing these systems. Strengthening such cross-regulatory mechanisms remains vital to closing enforcement gaps and ensuring worker protections evolve in tandem with the increasing intrusive digital management practices.

[223] Art. 19, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work COM(2021) 762 final.

[224] 'Towards Digital Clearinghouse 2.0: Championing a Consistent Supervisory Approach for the Digital Economy' (*European Data Protection Supervisor*, 15 January 2025) <https://www.edps.europa.eu/press-publications/press-news/blog/towards-digital-clearinghouse-20-championing-consistent-approach-digital-economy> accessed 1 April 2025.

[225] 'The Digital Regulation Cooperation Forum' (*GOV.UK*, 10 March 202AD) <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum> accessed 8 July 2022.

[226] 'The Digital Regulation Cooperation Platform (SDT)' <https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt> accessed 1 April 2025.

References

Abraha, H., "Regulating Algorithmic Employment Decisions through Data Protection Law" (2023) 14 European Labour Law Journal 172.

——, "A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace" (2022) 12 International Data Privacy Law 276.

Adams-Prassl, J. and others, "Regulating Algorithmic Management: A Blueprint" (2023) 14 European Labour Law Journal 124.

——, "Regulating Algorithmic Management: A Blueprint" (2023) 14 European Labour Law Journal 124.

Albin, E., "The Three-Tier Structural Legal Deficit Undermining the Protection of Employees' Personal Data in the Workplace" (2024) 45 Oxford Journal of Legal Studies 8.

"Algorithmic Management in Traditional Workplaces" (*Foundation for European Progressive Studies*) https://feps-europe.eu/publication/algorithmic-management-in-traditional-workplaces/.

Aloisi, A., and De Stefano, V., *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour* (Hart 2022).

ARTICLE 29 - Data Protection Working Party (2002), "Working document on the surveillance of electronic communications in the workplace", 5401/01/EN/Final WP 55

Ball, K., "Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations" (Publications Office of the European Union, JRC125716 2021)

Barros Vale, S., and Zanfir-Fortuna, G., "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities" (Future of Privacy Forum 2022).

Bodie, M.T., and others, "The Law and Policy of People Analytics" 88 U. COLO. L. REV.

Bogen, M., "All the Ways Hiring Algorithms Can Introduce Bias" *Harvard Business Review* (6 May 2019) https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias

Bogle, A., "Stop All Time Wasting": Woolworths Workers Tracked and Timed under New Efficiency Crackdown' *The Guardian* (22 October 2024).

"Bossware: The Dangers of High-Tech Worker Surveillance & How to Stop Them" (Big Brother Watch, September 19, 2024).

Bradford, A., *The Brussels Effect: How the European Union Rules the World* (Oxford Scholarship Online 2020).

Calacci, D., and Stein, J., "From Access to Understanding: Collective Data Governance for Workers" (2023) 14 European Labour Law Journal 253.

"Consumer Financial Protection Circular 2024-06: Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions" (*Consumer Financial Protection Bureau*, 24 October 2024)

Cox, D., "The Rise of Employee Health Tracking" (*BBC*, 11 November 2020)

Dastin, J., "Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women" *Reuters* (11 October 2018).

de Freitas Júnior, A. R., Zapolla, L. F., and Cunha, P. F. N., "The Regulation of Artificial Intelligence in Brazil" (2024) 77 ILR Review 869.

De Hert. P., and Lammerant, H., "Protection of Personal Data in Work-Related Relations" (European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2013).

"Decision of May 09, 2023 – 1 ABR 14/22" (*Das Bundesarbeitsgericht*, 9 May 2023) https://www.bundesarbeitsgericht.de/entscheidung/1-abr-14-22/.

Del Castillo, A. P., and Naranjo, D., "Regulating Algorithmic Management: An Assessment of the EC's Draft Directive on Improving Working Conditions in Platform Work" (ETUI Policy Brief 2022).

"Department of Labor Releases AI Best Practices Roadmap for Developers, Employers, Building on AI Principles for Worker Well-Being" (*DOL*, 16 October 2024).

Doellgast, V., and O'Brady, S., "Making Call Center Jobs Better: The Relationship between Management Practices and Worker Stress" [2020] Cornell University, ILR School

Jervis, C. E. M., "Barbulescu v Romania: Why There Is No Room for Complacency When It Comes to Privacy Rights in the Workplace" (*EJIL: Talk!*, 26 September 2017).

"Employee Monitoring: CNIL Fined AMAZON FRANCE LOGISTIQUE €32 Million" https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million

"Employee Monitoring Software" (*iMonitorSoft*) https://www.imonitorsoft.com/.

"Endorsed WP29 Guidelines" (*European Data Protection Board*) https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en.

Eurofound, *Employee Monitoring and Surveillance: The Challenges of Digitalisation* (Publications Office of the European Union, Luxembourg 2020)

——, "European Restructuring Monitor: Algorithmic Management" https://apps.eurofound.europa.eu/legislationdb/algorithmic-management

——, "European Restructuring Monitor: Employee Monitoring and Surveillance" https://apps.eurofound.europa.eu/legislationdb/employee-monitoring-and-surveillance

European Commission, "Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data" (2002)

——, "Staff Working Document SEC (2012) 72 Final"

European Commission Joint Research Centre, *The Platformisation of Work: Evidence from the JRC Algorithmic Management and Platform Work Survey (AMPWork).* (Publications Office of the European Union 2023) https://data.europa.eu/doi/10.2760/801282

European Framework Agreement on Digitalisation (BusinessEurope, SMEunited, CEEP and the ETUC 2020)

European Fundamental Rights Agency, "Data Protection in the European Union: The Role of National Data Protection Authorities" (Publications Office of the European Union, 2010)

Feng, K., "Overview of New Rights for Workers under the California Consumer Privacy Act" (*UC Berkeley Labor Center*, 6 December 2023) https://laborcenter.berkeley.edu/overview-of-new-rights-for-workers-under-the-california-consumer-privacy-act/

"For Your Information: Australian Privacy Law and Practice (ALRC Report 108) Vol.1" (Australian Law Reform Commission 2008) https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

"For Your Information: Australian Privacy Law and Practice" (Australian Law Reform Commission (Vol 2, Report 108) 2008)

Francis, J., "Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends" (FPF US Legislation Report 2024) https://fpf.org/blog/fpf-unveils-report-on-the-anatomy-of-state-comprehensive-privacy-law/

Freedland, M., *Data Protection and Employment in the European Union: An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and Its Member States* (European Commission 1999)

Garden, C., "Labor Organizing in the Age of Surveillance" (2018) 63 St. Louis U. L.J.

Gary, T. M., and Sherizen, S., "Monitoring on the Job: How to Protect Privacy as Well as Property" (*Technology Review*, 1986) https://web.mit.edu/gtmarx/www/privacy.html

"Genetic Information Discrimination" (*US EEOC*) https://www.eeoc.gov/genetic-information-discrimination

"Germany Draft for Employee Data Act Issued" (*www.hoganlovells.com*, 29 October 2024) https://www.hoganlovells.com/en/publications/germany-draft-for-employee-data-act-issued

Ghaffary, S., "The Real Cost of Amazon" (*Vox*, 29 June 2020) https://www.vox.com/recode/2020/6/29/21303643/amazon-coronavirus-warehouse-workers-protest-jeff-bezos-chris-smalls-boycott-pandemic

"Government Response to the Privacy Act Review Report" (Attorney-General's Department 2023) https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

Greenleaf,G., "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills" [2023] SSRN Electronic Journal https://www.ssrn.com/abstract=4426146

Gurley, L. K., "Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts" (*VICE*, 2 June 2022) https://www.vice.com/en/article/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts/

Hendrickx, F., "Protection of Workers' Personal Data: General Principles" (ILO Working Paper 62 2022)

Hießl, C., "Jurisprudence of National Courts in Europe on Algorithmic Management at the Workplace" (European Centre of Expertise in the field of labour law, employment and labour market policies (ECE) 2023)

Hilliard, A., Guenole, N., and Leutner, F., "Robots Are Judging Me: Perceived Fairness of Algorithmic Recruitment Tools" (2022) 13 Frontiers in Psychology 940456

Holland, P., "Workplace Biometric: Major Weaknesses in Protecting Employee Privacy (Submission Privacy Act Review – Discussion Paper)" https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/view_respondent?_b_index=0&uuId=457461490

"How Independent Are African Data Protection Authorities?" (*Data Protection Africa | ALT Advisory*, 28 June 2023) https://dataprotection.africa/standing-alone-the-independence-of-african-data-protection-authorities/

Hu, J., "99% of Fortune 500 Companies Use Applicant Tracking Systems" (*Jobscan*, 7 November 2019) https://www.jobscan.co/blog/99-percent-fortune-500-ats/

IAPP, "US State Privacy Legislation Tracker: Introduced in the 118th Congress (2023-2024)" https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

ILO, "Improving Workers' Data Rights" (ILO brief 1 2022) https://www.ilo.org/publications/improving-workers-data-rights

"Interdisciplinary Council on Employee Data Protection" https://www.denkfabrik-bmas.de/en/topics/employee-data-protection/interdisciplinary-council-on-employee-data-protection

Kantor, J., and others, "The Rise of the Worker Productivity Score" *The New York Times* (15 August 2022) https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html

Lecher, C., "How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'" (*The Verge*, 25 April 2019) https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

Lee, J. B., and others, "A Privacy and Employment Law Primer: Recent Updates on Discrimination and Privacy Implications of Technology in the Workplace" (August 2022)

Leon, H., "Whole Foods Secretly Upgrades Tech to Target and Squash Unionizing Efforts" (*Observer*, 24 April 2020) https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/

——, "Whole Foods Secretly Upgrades Tech to Target and Squash Unionizing Efforts" (*Observer*, 24 April 2020) https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/

Mosendz, P., and Melin, A., "Bosses Are Panic-Buying Spy Software to Keep Tabs on Remote Workers" (*Los Angeles Times*, 27 March 2020) https://www.latimes.com/business/technology/story/2020-03-27/coronavirus-work-from-home-privacy

Neeser, R., "Brazil Data Protection Law – Litigation in the Context of Employment" (26 February 2024) https://www.littler.com/news-analysis/asap/brazil-data-protection-law-litigation-context-employment

"NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices" (*National Labor Relations Board*, 31 October 2022) https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and

"NLRB Memo Takes Aim at Intrusive Workplace Surveillance & Algorithmic Management Systems" (*Center for Democracy and Technology*, 21 December 2022) https://cdt.org/insights/nlrb-memo-takes-aim-at-intrusive-workplace-surveillance-algorithmic-management-systems/ accessed 1 May 2025

Nogarede, J., "No Digitalisation without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace" (FEPS Policy Study, November 2021)

Nogarede, J., Silberman, M., and Bronowicka, J., "Improving Workplace Data Protection: Achieving Workplace GDPR Compliance, Clarifying National Workplace Data Protection Rules, and Enhancing Worker Data Protection through Social Dialogue" (Friedrich-Ebert-Stiftung 2024)

O'Neal, M. N., "The Effects of Productivity Tracking on Employees" (*Indeed Career Guide*) https://www.indeed.com/career-advice/career-development/effects-productivity-tracking-employees

"Open Letter to President Biden from Tech Workers in Kenya" (*Foxglove*) https://www.foxglove.org.uk/open-letter-to-president-biden-from-tech-workers-in-kenya/

"Personal Privacy in an Information Society" (US Privacy Protection Study Commission 1977)

Portela, J. V. C., "Regulatory framework for artificial intelligence passes in Brazil's Senate" (*Mattos Filho*, 11 December 2024) https://www.mattosfilho.com.br/en/unico/framework-artificial-intelligence-senate/

"Privacy Act Review – Discussion Paper" (Submission by the Office of the Australian Information Commissioner 2020) https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-4-exemptions

"Privacy Act Review Report 2022" (Australian Government Attorney General's Department)

"Privacy (and Technology) in Workplaces: A Brief Overview of Brazilian Law and Practices to Ensure Employee Privacy" https://www.dentons.com/en/insights/articles/2023/february/24/a-brief-overview-of-brazilian-law-and-practices-to-ensure-employee-privacy

"Published Responses for Privacy Act Review – Discussion Paper" (- *Attorney-General's Department*) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent?_b_index=120

"Quarterly Notice N°01-2023 of the Senegal Personal Data Protection Commission (CDP)" https://www.cdp.sn/content/avis-trimestriel-n%C2%B001-2023-de-la-commission-de-protection-des-donnees-personnelles-du-0

Rani, U., Pesole, A., and González Vázquez, I., "Algorithmic Management Practices in Regular Workplaces: Case Studies in Logistics and Healthcare" (Luxembourg: Publications Office of the European Union, 2024)

Ravid DM and others, 'EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring' (2020) 46 Journal of Management 100

Reicin, E., "AI Can Be A Force For Good In Recruiting And Hiring New Employees" (*Forbes*, 16 November 2021) https://www.forbes.com/sites/forbesnonprofitcouncil/2021/11/16/ai-can-be-a-force-for-good-in-recruiting-and-hiring-new-employees/

Rhea, A., and others, "Resume Format, LinkedIn URLs and Other Unexpected Influences on AI Personality Prediction in Hiring: Results of an Audit", *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society* (ACM 2022) https://dl.acm.org/doi/10.1145/3514094.3534189

Riso, S., "Monitoring and Surveillance of Workers in the Digital Age" (Eurofound) https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age

Riso, S., and Litardi, C., "Employee Monitoring: A Moving Target for Regulation" (*Eurofound*, 15 July 2024) https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation

Rosenblat, A., and Stark, L., "Uber's Drivers: Information Asymmetries and Control in Dynamic Work" [2015] SSRN Electronic Journal http://www.ssrn.com/abstract=2686227

Sainato, M., '"You Feel like You'Re in Prison': Workers Claim Amazon's Surveillance Violates Labor Law" *The Guardian* (21 May 2024) https://www.theguardian.com/us-news/article/2024/may/21/amazon-surveillance-lawsuit-union

Schwartz, Jr. R. G., "Privacy in German Employment Law" (1992) 15 Hastings Int'l & Comp. L. Rev

Scott, G., "Labor Organizing and AI Surveillance in the Workplace" (*George Town Journal on Poverty Law & Policy*, 14 January 2024) https://www.law.georgetown.edu/poverty-journal/blog/labor-organizing-and-ai-surveillance-in-the-workplace/

"Senegal: CDP Releases Guidance on Processing of Biometric Data in the Workplace" (*DataGuidance*) https://www.dataguidance.com/news/senegal-cdp-releases-guidance-processing-biometric-data

Simitis, S., "Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data" (1999) 5 European Law Journal 45

Stanley, J., "Amazon Drivers Placed Under Robot Surveillance Microscope" (*American Civil Liberties Union*, 23 March 2021) https://www.aclu.org/news/privacy-technology/amazon-drivers-placed-under-robot-surveillance-microscope

Stockburger, P., "Privacy in the US Workplace – a Rapidly Changing Legal Landscape" (*DENTONS*, 16 February 2023) https://www.dentons.com/en/insights/articles/2023/february/16/privacy-in-the-us-workplace-a-rapidly-changing-landscape

"Submissions - Inquiry into Workplace Surveillance" (*Parliament of Victoria*) https://www.parliament.vic.gov.au/get-involved/inquiries/inquiryintoworkplacesurveillance/submissions/

Susskind, J,. *The Digital Republic: On Freedom and Democracy in the 21st Century* (Pegasus Books 2022)

——, *The Digital Republic: On Freedom and Democracy in the 21st Century* (Bloomsbury Publishing 2022)

Taylor, F. W., *The Principles of Scientific Management* (Dover Publications 1997)

"The Algorithm That Tells the Boss Who Might Quit...Wal-Mart, Credit Suisse Crunch Data to See Which Workers Are Likely to Leave or Stay" https://www.firstsun.com/2015/03/18/strategy-the-algorithm-that-tells-the-boss-who-might-quit-wal-mart-credit-suisse-crunch-data-to-see-which-workers-are-likely-to-leave-or-stay/

"The Digital Regulation Cooperation Forum" (*GOV.UK*, 10 March 202AD) https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum

"The Digital Regulation Cooperation Platform (SDT)" https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt

"The Electronic Supervisor: New Technology, New Tensions" (US Congress, Office of Technology Assessment, September 1987)

Todolí-Signes, A., "Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection" (2019) 25 Transfer: European Review of Labour and Research 465

"Towards Digital Clearinghouse 2.0: Championing a Consistent Supervisory Approach for the Digital Economy" (*European Data Protection Supervisor*, 15 January 2025) https://www.edps.europa.eu/press-publications/press-news/blog/towards-digital-clearinghouse-20-championing-consistent-approach-digital-economy

Townsend, P., "Data Privacy Is Not Just a Consumer Issue: It's Also a Labor Rights Issue" (*Next100*, 14 May 2020) https://thenext100.org/data-privacy-is-not-just-a-consumer-issue-its-also-a-labor-rights-issue/

Tsebee, D., and Oloyede, R., "Roundup on Data Protection in Africa 2023" (Tech Hive 2023)

——, "State of AI Regulation in Africa: Trends and Developments" (Tech Hive 2024)

——, "DPAs and AI Regulation in Africa" https://iapp.org/news/a/dpas-and-ai-regulation-in-africa accessed 14 November 2024

UNICE, "Commission's Second-Stage Consultation on the Protection of Workers' Personal Data" (6 January 2003)

United Workers Union, "Technology and Power: Understanding Issues of Insecure Work and Technological Change in Australian Workplaces" (2020)

U.S. Equal Employment Opportunity Commission, "The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees" https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence

"US State-by-State AI Legislation Snapshot" (*BCLP*) https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html

West, D. M., "How Employers Use Technology to Surveil Employees" (*Brookings*, 5 January 2021) https://www.brookings.edu/articles/how-employers-use-technology-to-surveil-employees/

Wheeler, M. A., "Does Tracking Your Employees Actually Make Them More Productive?" (*The Conversation*, 24 October 2024) http://theconversation.com/does-tracking-your-employees-actually-make-them-more-productive-242027

"Which African Countries Have a Data Protection Law?" (*Data Protection Africa | ALT Advisory*, 14 November 2023) https://dataprotection.africa/which-african-countries-have-a-data-protection-law/

Whittaker, M., and others, "Disability, Bias, and AI – Report" (AI Now Institute 2019) https://ainowinstitute.org/publication/disabilitybiasai-2019

Williams, A., Miceli, M. and Gebru, T., "The Exploited Labor Behind Artificial Intelligence" (*NOEMA*, 13 October 2022) https://www.noemamag.com/the-exploited-labor-behind-artificial-intelligence

"Workers' Privacy Part II: Monitoring and Surveillance in the Workplace" (International Labour Office, Conditions of work digest, Vol 12 Number 1, 1993)

"Workers' Privacy Part I-Protection of Personal Data" (International Labour Office, Conditions of work digest, Vol 10 Number 2, 1992)

"Workplace Privacy in US Federal and State Laws and Policies | IAPP" (*IAPP*) https://iapp.org/news/a/workplace-privacy-in-us-laws-and-policies

Xiang, C., "OpenAI Used Kenyan Workers Making $2 an Hour to Filter Traumatic Content from ChatGPT" (*VICE*, 18 January 2023) https://www.vice.com/en/article/openai-used-kenyan-workers-making-dollar2-an-hour-to-filter-traumatic-content-from-chatgpt/

Zanatta, R. A. F., and Rielli, M., "The Artificial Intelligence Legislation in Brazil: Technical Analysis of the Text to Be Voted on in the Federal Senate Plenary" (*Data Privacy Brasil Research*, 10 December 2024) https://www.dataprivacybr.org/en/the-artificial-intelligence-legislation-in-brazil-technical-analysis-of-the-text-to-be-voted-on-in-the-federal-senate-plenary/

Bărbulescu v Romania [2017] ECtHR 61496/08

Case C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums ECLI:EU:C:2023:270

Jeremy Lee v Superior Wood Pty Ltd [2019] FWCFB 2946 (1 May 2019)

Rechtbank Amsterdam, Case C/13/687315 / HA RK 20-207, ECLI:NL:RBAMS:2021:1020, March 11, 2021

Regional Administrative Court of Hannover, Case 10 A 6199/20 February 8, 2023

AB-1651 Worker rights: Workplace Technology Accountability Act.(2021-2022)

Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017

Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48

Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context (WP 48) 13 Sept 2001

Article 29 Working Party Opinion 2/2017 on data processing at work (WP 249) 8 June 2017

Article 29 Working Party Opinion 2/2017 on data processing at work (WP 249) 8 June 2017

Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, October 2022

California Code, Labor Code - LAB § 435

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions− A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final

Council of Europe Explanatory Memorandum to Recommendation No. R (89) 2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes (Adopted by the Committee of Ministers on 18 January 1989)

Digital Personal Data Protection Act 2023

Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community - Joint declaration of the European Parliament, the Council and the Commission on employee representation

Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes 2024

Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0 Adopted on 8 October 2024)

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0, Adopted on 8 October 2024)

HB24-1130-Concerning Protecting the Privacy of an Individual's Biometric Data

HB3773 -The Illinois Human Rights Act

H.R.7621 - No Robot Bosses Act, 118th Congress (2023-2024)

H.R.7690 - Stop Spying Bosses Act, 118th Congress (2023-2024)

H.R.8818 - American Privacy Rights Act of 2024, 118th Congress (2023-2024)

Illinois Artificial Intelligence Video Interview Act 2020

Illinois Biometric Information Privacy Act 2008

ILO code of practice on the Protection of workers' personal data 1997

Local Law 144 of 2021, Automated Employment Decision Tools (AEDT)

New York Consolidated Laws, Labor Law - LAB § 203-c

Privacy and Other Legislation Amendment Act 2024 (NO. 128, 2024)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work COM(2021) 762 final

Proposal for the DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work 7212/24 ADD 1

Protection of Personal Data Act 2023

Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes 1989

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

S.2440 - Exploitative Workplace Surveillance and Technologies Task Force Act of 2023, 118th Congress (2023-2024)

S.3238 - Privacy for Consumers and Workers Act 102nd Congress (1991-1992)

West Virginia's Electronic surveillance Act, Sec 21-3-20

Acknowledgements

Special thanks to Antonio Aloisi (IE University Law School in Madrid), Jeremias Adams-Prassl (Oxford), Michael 'six' Silberman (Oxford), Elizabeth Coombs (University of Malta), Ketan Modh (Deloitte India), Janine Berg (ILO), Anne Boyd (ILO) and Caroline Fredrickson (ILO).

Advancing social justice, promoting decent work

The International Labour Organization is the United Nations agency for the world of work. We bring together governments, employers and workers to improve the working lives of all people, driving a human-centred approach to the future of work through employment creation, rights at work, social protection and social dialogue.

Contact details

Research Department (RESEARCH)

International Labour Organization
Route des Morillons 4
1211 Geneva 22
Switzerland
T +41 22 799 6530
research@ilo.org
www.ilo.org/research

ISBN 9789220426326