Chapter 13
Worker monitoring vs worker surveillance: the need for a legal differentiation

Aída Ponce Del Castillo and Michele Molè

1. Introduction

In recent years, the use of increasingly powerful technologies to monitor workers has become a prevalent and almost ubiquitous feature of the labour market. These technologies are used for a variety of purposes including monitoring productivity, measuring workers' performance, tracking movements and workers' health, and making profiles of the workforce used for multiple purposes. They have permeated all types of workplaces and sectors. No job, task, profession or sector is immune to this intrusive practice which reduces workers to a 'quantified self' (Lupton 2016; Moore 2018; Swan 2013). It can extend beyond the confines of the workplace, working time and one's working life (Hendrickx 2018). Against this background, the European Social Partners, as delineated in their Autonomous Framework Agreement on Digitalisation (2020), have identified worker surveillance as a pivotal topic for social dialogue.

The objective of this chapter is to point to the increasing interest in workers' permanent measurement provided by new surveillance products. It provides factual and legal arguments that support the need to draw a line between the concept of 'worker monitoring' and 'worker surveillance', arguing that such surveillance creates a situation of structural asymmetry between employers and workers in terms of information and control at work, while also leading to abuses of workers' rights. Against this background, it highlights the need to set boundaries to employers' monitoring prerogatives, themselves significantly enhanced by the development of new and powerful surveillance technologies. The analysis is based on literature from sociology, surveillance studies and law.

Section 2 describes the right of employers to monitor the workforce under the European Convention on Human Rights (ECHR). Although this monitoring power is governed by the principles of proportionality and necessity set down in Article 8 ('Right to respect for private and family life'), it contends that the rapid advance of technology and its promises has provided employers with an intrusive and invisible, yet intensive, monitoring power which should not find the European legal framework on worker monitoring unprepared.

Section 3, after describing how worker monitoring has evolved and transformed into surveillance, takes a closer look at the recent decisions taken by national data protection authorities (DPAs) and argues that privacy in the workplace is an issue that should more consistently be on their radar. It looks at the impact of surveillance on occupational safety and health, and argues that this has led to a gradual erosion of the principle and culture of prevention. Section 4 addresses data, the driving force behind worker surveillance, and data analysis.

Section 5 lays the groundwork for a legal definition: it shows how surveillance can be considered an unnecessary monitoring power of the employer which often fails the suitability and necessity tests as developed by the jurisprudence of the European Court of Human Rights (ECtHR). Then this chapter concludes.

2. The monitoring power of employers: an open contractual clause

The right to monitor employees is one of the essential powers granted to employers 'to ensure the smooth running of the company', a concept discussed in the ECtHR landmark case *Bărbulescu v. Romania* (2017) (which went on to rule that the monitoring of an employee's corporate messaging account was a violation of the right to respect for private life and correspondence under Article 8 of the ECHR). Such a power includes a variety of monitoring activities covered by an employer's right to property and to conduct a business (Art. 16 and Art. 17 Charter of Fundamental Rights of the European Union (CFREU); Art. 1 ECHR Protocol 1). Managing an economic activity is linked with the legal and legitimate interest of the employer to oversee any work-related activity: company organisation; employee performance; compliance with occupational safety and health (OSH) laws; and protection of company assets. Therefore, the monitoring power of the employer is an implicit clause of the employment contract, defined here as a contractual clause that does not set specific details about the intensity, quality or pace of the monitoring that the employer will perform. Thus, in the contract, the employer has the ability to monitor the workforce with few limitations, allowing for direct or technology-based observation, e.g. cameras, sensors, geolocation systems or device tracking by default (such as laptops, smartphones, etc.) (Ball 2010; Carby-Hall 2003: 34; Coase 1937).

Such an employer power finds, however, either restrictive or permissive regulatory approaches in the various European Member States. As noted by Eurofound, legislative interventions on employer discretion in monitoring are focused, at national level, mainly on two purposes: they legitimise monitoring for occupational safety and health or security purposes; while they prohibit (or link to transparency duties) the direct monitoring of the employee's work performance (Riso 2020: 8-16).

A similar approach to limiting employer discretion comes from the European Court of Human Rights. With the *Niemietz* case (*Niemietz v. Germany*, 1992) came the first reference to the protection of an employee's privacy and personal data under the scope of Article 8 ECHR. Mr Niemietz was a lawyer who complained before the ECtHR that a search of his offices was an interference with his private life. There, the Court held that there exists in a workplace an individual right to personal development and to establish relationships with other individuals; a sphere that cannot be disproportionately reduced to accommodate an employer interest in monitoring.

Thereafter, the Court has addressed diverse and specific implementations of this monitoring power. Monitoring via cameras or GPS has often been found to be legitimate for preventing theft or the abuse of company property (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022; *López Ribalda and Others v. Spain*, 2019; *Köpke v. Germany*, 2010). In these cases, monitoring systems had been (legitimately) implemented to prevent the illegitimate use of a company car through GPS tracking (*Florindo*, 2022) or to provide video evidence of the theft of goods or money by shop assistants (*López Ribalda*, 2019; *Köpke* 2010). However, the scope of the power has often been found to contravene the right to privacy when cameras or other tracking systems have been employed to monitor an employee's work performance (*Antović and Mirković v. Montenegro*, 2018; *Bărbulescu v. Romania*, 2017; *Copland v. United Kingdom*, 2007; *Halford v. UK*, 1997). In *Antović and Mirković v. Montenegro* (2018), Ms Antović and Mr Mirković alleged that the unlawful installation and use of video surveillance equipment in the university auditoriums where they held classes had violated their right to respect for their private life. Similarly for Mr Bărbulescu's Yahoo Messenger account: opened for business purposes, this was monitored by his employer including his personal and non-professional communications. In the cases involving Ms Copland and Ms Halford, their right to private life was, according to the Court, disproportionately reduced by the covert monitoring of email and internet use (*Copland*, 2007) and of telephone conversations (*Halford*, 1997).

Looking through the ECtHR's rulings on worker monitoring, two principles set boundaries on a case-by-case basis to the 'openness' of the monitoring power: necessity and proportionality. The Court weighs the proportionality of the intrusion into the private sphere of employees against the right of employers to manage and preserve their economic activity. In addition, the practical implementation of the monitoring measure is also assessed: according to the principle of necessity, the employer must adopt the most suitable and least intrusive measures to express its legitimate interest in monitoring (Gerards 2013). The principles of proportionality and necessity of the monitoring measure are also reflected in Art. 5 GDPR ('Principles relating to processing of personal data'). Yet, the European Court of Justice (ECJ) has still not dealt with the monitoring power of employers and the application of the GDPR's principles (Mangan 2022: 321).

3. The transformation of monitoring into surveillance

As described above, there is extensive ECtHR jurisprudence on monitoring and privacy at work. Today, however, we are witnessing a gradual transformation of monitoring into surveillance, a process characterised by the acquisition of new features and purposes: employers use monitoring technologies that go beyond those analysed so far by the courts, such as video surveillance, GPS, biometric scans or tools that allow access to personal communications (Zuboff 2019). Powerful new technologies are creating new challenges for courts as to what can be considered proportionate and necessary in the digital age. Increasingly, labour scholars are calling for a 'technological contextualisation' of labour regulation in light of the rapid expansion of the market for workplace surveillance technologies which threatens the enjoyment of fundamental rights at work (Aloisi and De Stefano 2022; Mangan 2022; Molè 2022).

This chapter refers to this new form of all-encompassing monitoring as ‘worker surveillance’ and argues that it operates on the basis of ‘the three Is’: it is intrusive on and invisible to the individuals it targets; and is characterised by the intensive collection of data.

The sociologist Gary T. Marx defines surveillance in the *International Encyclopedia of the Social & Behavioral Sciences* as the ‘scrutiny of individuals, groups, and contexts through the use of technical means to extract or create information’ (Marx 2015). In a post Covid-19 context, this definition remains valid, but the phenomenon has undergone exponential growth. It now operates on a practically limitless scale and generates constant and substantial amounts of fine-grained personal and sensitive data. Modern surveillance tools capture data points related to the worker’s emotional state (anxiety, frustration, boredom, happiness, fear, insecurity, etc); safety (exposure to hazards, risk levels, movements, fatigue, microsleep episodes, etc); health (physiological data such as heart rate, blood pressure, breathing rate, temperature, ergonomic data such as ‘good’ or ‘bad’ posture, stress levels, possible burnout, etc.) (Al Jassmi et al. 2019; Jebelli et al. 2019; Moore 2018; Swan 2013); wellness (sleep patterns, fatigue management, level of physical activity, etc) (Dockser Marcus 2023); brain activity (Cheng et al. 2022; Farahany 2023; Wang et al. 2017); security (use of company assets, information leaks, risky behaviours, etc); and productivity (engagement with teammates, working time vs rest time, contents of e-mails, internet use, etc.) (Burnett and Lisk 2021). The collected data is then measured, analysed and processed for a variety of purposes.

Surveillance tools and techniques are often invisible and non-material, embedded within other technologies and devices. This, coupled with the broad range of data points collected, makes worker surveillance a markedly distinct practice from monitoring. As briefly anticipated in Section 2, a legal differentiation following the transformation of monitoring into surveillance has become imperative.

The gradual shift from monitoring to surveillance can be primarily attributed to technological advance and the enhanced capacity to gather data. First, the advent of new software, tools and technology considerably expanded the scope, until then relatively limited, of human resource management (HRM) (Gallup 2023; Laker et al. 2020). This led to the emergence of people analytics (PA), which HRM experts describe as a data-driven method analysing all the processes related to personnel in a company with the aim of achieving business success and increasing the organisation’s efficiency and productivity (De Cremer and Stollberger 2022). The next generation of tools incorporated novel AI-based models to enable even more intricate surveillance and provide employers with more powerful insights in decision-making. These tools are used to assist managers when allocating rewards (salary rises, promotions) or imposing disciplinary measures (dismissals, suspensions of platform accounts, etc.).

The latest tier in this hierarchy of monitoring techniques is algorithmic management (AI Now Institute 2023), or automated monitoring and decision-making systems. Through the use of third parties, vendors, networks, data brokers and transfer mechanisms, the power of the employer to process workers' data has dramatically increased. Surveillance tools not only capture data, to be processed and used by managers, but they can also be used to support decisions (Adams-Prassl 2019).

Algorithmic management is one of the building blocks of the platform business model (Stark and Pais 2020) and it is gradually encroaching on more traditional forms of employment. The proposed directive on improving working conditions in platform work aims to regulate automated decision-making and monitoring systems in the platform economy (European Commission 2021), but several challenges remain – especially when used in standard employment settings. These include the overall opacity of existing processes, the metrics employed, the implications of collecting data in nanoseconds, the use of surveillance techniques in determining workers' employability and the impact of behavioural analytics on workers' remuneration but which – as also noted by Bales and Stone (2020) – deter unionisation, enable subtle forms of employer blackballing, exacerbate employment discrimination, render trade unions ineffective and eradicate the protections of labour law.

3.1 Privacy and data protection in the workplace: a new issue of concern for data protection authorities

The Covid-19 pandemic brought the issue of worker surveillance into the spotlight and captured the attention of both the general public and the workforce. With companies wanting to monitor workers physically absent from the workplace, the use of analytical tools intensified. Surveillance became more prevalent, justified on the grounds of productivity and safety (Ball 2010), and started to be employed for a multiplicity of purposes going beyond workers' 'data perimeter' as identified by Mario Guglielmetti (this volume). Instances of misuse became frequent, as data collected from workers was used to penalise and discipline them, as well as to automate decisions that had adverse effects on them (Agosti et al. 2023; Rogers 2023). Against this backdrop, it is essential to consider whether the obligation to conduct a data processing impact assessment under Article 35 of the GDPR, involving the participation of worker representatives, has been adequately met.

Privacy in the workplace became an issue on the radar of national DPAs. Several issued recommendations to employers about the collection of data on remote workforces. In the UK, the Information Commissioner's Office (ICO)I reminded employers that, prior to starting processing, they must first assess whether the use of artificial intelligence (AI) is a necessary and proportionate solution to a problem (ICO 2022). In France, Commission Nationale Informatique & Libertés (CNIL; National Commission for Information Technology and Liberties) highlighted the existence of a particularly invasive piece of software which, when used, leads to a permanent and disproportionate surveillance of employees' activities. L'Autorité de protection des données/Gegevensbeschermingsautoriteit (APD/GBA; the Belgian DPA) reminded of the general prohibition on using cameras with AI to monitor the workforce.

In some cases, companies have been fined for excessive monitoring, including H&M's Service Centre (35 million euros) and notebooksbilliger.de (10.4 million euros), both in Germany (European Data Protection Board 2020a, 2020b).

Similarly, the Italian DPA fined the food delivery platform Foodinho 2.6 million euros, finding that 'the company had failed to adequately inform its employees on the functioning of the system and had not implemented suitable safeguards to ensure accuracy and fairness of the algorithmic results that were used to rate riders' performance' GPDP 2021). In other words, the Italian DPA questioned the covert surveillance and meaningfulness of the measurements carried out by the company regarding employees' activities: it found the data collected to be not relevant and used for discriminatory purposes, including communications in chats, emails and phone calls between couriers and customer care. Furthermore, technical evidence revealed that, when the mobile app was running in the background, it continued to send notifications of unassigned orders to all couriers, even those not on shift. It processed couriers' GPS location continuously and automatically – without verifying the actual need for such processing; sent data to the platform on the exact location of a courier, the speed and mobile phone battery level; and shared data, including GPS location, personal login, name and the courier's unique identifier, with third parties. It also produced a 'hidden' score for the courier, with no clear indication of the purpose of this value (Agosti et al. 2023).

Another relevant case is CNIL's investigation into the collection and analysis by Amazon France Logistics of data on its employees. In this case, Amazon was investigated on two indicators: 'the machine gun', which is the amount of time in which the worker puts away an item in less than 1.25 seconds; and 'idle time', when the worker does not store an item for 10 minutes. The CNIL has requested a fine of 170 million euros (Vitard 2023).

That DPAs are aware of the significant issue represented by privacy in the workplace is a welcome evolution. However, many types of surveillance practices continue to exist without being detected by any authority. In improving the enforcement of the GDPR, DPAs and labour authorities could intensify their level of cooperation, become allies and cross-fertilise their respective activities.

3.2 The impact of surveillance on occupational health and safety: a gradual erosion of prevention

One of the workplace dimensions most targeted by surveillance technologies has been occupational safety and health. Companies are increasingly resorting to technology not only regarding various aspects of their operations and work organisation but for the purposes of primary prevention and risk reduction as well as a mechanism for compliance with OSH legislation. Relying on the data of workers that that should not be being processed by the employer in the first instance, thereby trespassing workers' data perimeter, marketing strategies often feature promises such as 'streamline your safety processes and help create a culture of safety' (www.fluix.com); observing that 'automated prediction programs allow construction employees to minimize errors during calculation, errors that could have created real risk during the building process' (www.kreo.net); while some seek to substitute the role of safety staff – 'by automating the repetitive and mundane aspects of the safety and health inspection, Intenseye enables safety inspectors and customers to utilize their skills for problem-solving while providing them with the relevant information regarding the problems' (www.intenseye.com). The promise is clear that sensors, cameras, IoT (internet of things) devices and AI systems can be promoted as tools that vigilantly monitor workplaces in real time, predicting potential risks, recognising unsafe behaviours, detecting unsafe conditions and suggesting recommendations to mitigate potential risks (Malik 2023; van Rijmenam 2023).

Even when AI systems could be helpful in risk management, the reliance on them needs to be carefully weighted since trusting in techno-solutions can embody a questionable shift of approach. The promotion of a culture of prevention, based on the active participation of and cooperation between managers, workers and their representatives, is a principle recognised and promoted by the International Labour Office in Convention 186 and enshrined in the European Framework Directive on Safety and Health at Work. Evidence shows that the effectiveness of safety management systems depends on a collective and positive health and safety culture that steers work towards optimising workers' physical and mental health (Wadsworth and Walters 2019; Nielsen 2014; Menéndez et al. 2009).

Following Gould (this volume), this chapter argues that technology-based surveillance is being pursued as another face of technology solutionism which finds it difficult to comprehend the reality of work, human factors and associated uncertainties. It not only goes beyond workers' 'data perimeter' but is increasingly being mistaken for, while also replacing, the culture of prevention that underpins occupational safety and health. Instead of establishing a cooperative and dynamic prevention culture, companies are opting for a 'machine-based' approach to 'advise', 'recommend', 'help' or even 'prevent' risks from materialising.

When using technology to pursue occupational safety and health, privacy is often not only seen as a trade-off but is quickly traded away. Yet privacy, and data protection, are an integral element of the right to health and to being safe, as well as a dimension of human integrity and ultimately human dignity, the foundation of all fundamental rights. The interconnection between health, safety, wellbeing and privacy is inseparable. Against such a backdrop, EU-OSHA, the European Agency for Safety and Health at Work, appears to endorse the use of automated measurement systems (comprising sensors, smart personal protective equipment, virtual and augmented reality, drones, etc.) to detect, minimise or eliminate risks (EU-OSHA 2023). The Agency has compiled eight case studies that exemplify how advanced robotics and AI-based systems can be used to automate physical and cognitive tasks in the workplace (EU-OSHA 2023).

Although an approach which sets out to minimise risks seems to be welcome, there are several implications to consider.

First, following Hildebrandt (2023), the automation of practices and even norms is a growing trend. There is an implicit validation of technology-based solutions that are being marketed to pursue preventive purposes, but without due diligence being undertaken in verifying design choices; identifying how well they fulfil their claims, functionalities and potential uses described in the terms of use; establishing how far they are reliable, effective or even helpful; and labelling their associations with third parties. As Hildebrandt (2022) sums up, 'the relevance of the solution always depends on purpose, context and agents'.

Second, the use of 'all-in-one' solutions which serve multiple purposes contradicts the coexistence of various fundamental legal dispositions. It moves away from a comprehensive approach to conducting risk assessments, characterised as a 'collaborative practice'. As various authors have observed, employers can, in their duty to assess risks systematically, work in collaboration with workers, their representatives and other experts in seeking to enhance worker protection encompassing diverse perceptions of risks, reviewing both qualitative and quantitative data and considering the variety of hazards and their severity (Castro and Ramos 2017; EU-OSHA 2007; Frick 2011, Ollé-Espluga et al. 2015). Also, as discussed in Section 2, it contravenes the core principles of necessity (assessment of the effectiveness of the measure in relation to the objective pursued) and proportionality (assessment of the appropriateness of the extent to which there is a logical link between the measure and the legitimate objective pursued) (EDPS 2019). Additionally, solutions often justify their deployment through ethical principles and rely on the consent of workers,[1] inadvertently disregarding that, when processing workers' personal data, often of a sensitive nature, informed consent does not constitute a lawful legal basis for such data processing (Article 29 Data Protection Working Party 2017).

Third, the risks associated with this situation are numerous both at individual and collective levels. Workers' autonomy and decision-making power, their capacity to be critical towards the use of technology and their capacity to bargain collectively can all be eroded (Hendrickx 2018). Its use may also conceal workers' tacit knowledge of their working environment and be a cause of deskilling and a reduction of agency.

One must also consider the implications for safety representatives and labour inspectors in this new environment. Despite the obligations under the Framework Directive, legal challenges have also been made related to liability and accountability in the event of system failures or accidents. This may provide some employers with the means to evade liability by shifting blame to the victim for non-compliance with safety rules or any failure to follow system recommendations, or otherwise by attributing the mistake to the system itself.

At work organisation level, the reliance on AI systems within intricate interconnected environments involving various actors such as employers, employees, technology providers, vendors and third parties may dilute the culture of prevention. Exposure to

[1] For example, Intenseye's Ethics Principles state that: 'Intenseye requires its users to deploy their technology responsibly, clearly informing workers and limiting their use of technology to its intended and justified goals' https://www.intenseye.com/company/ai-ethics-statement

technologies that automate OSH objectives can have adverse effects on workers' overall health and wellbeing (Cabrelli and Graveling 2019; Schulte et al. 2020). An overly mechanical approach to prevention may prove less adaptive to changes in the working environment.

Machine-based prevention systems can, furthermore, lead to a fragmentation of organisational processes and damage the very purpose of occupational safety and health. Even when the Framework Directive provides for the employer to take the measures necessary for the safety of employees and the protection of their health, including the prevention of occupational risks, a reliance on AI systems might be questionable. AI systems depend heavily on the quality of data and the robustness of the predictive AI models they use. Conversely, one of its weakness comes from weak variables, the unpredictability of the external environment and the diversity and unpredictability of the 'human factors' and inputs which, if inadequately taken into account, can put occupational health and safety at risk (Badri et al. 2018; Reiman et al. 2021). AI systems are prone to inheriting inductive bias related to their training data, as well as to ethical and unlawful bias (Brynjolfsson et al. 2023; Hildebrandt 2023). If not carefully designed and monitored continuously, these systems may perpetuate or even exacerbate existing biases and discrimination in the workplace. In the process, OSH risks being transformed from a 'safety practice' into an 'ethical practice' or, worse, a compliance exercise.

Finally, it is imperative to stress the interconnectedness of health, safety, privacy and other human dimensions. Measuring and analysing them in isolation leads to fragmentation, undermining human integrity, dignity and the protection of fundamental rights. Prevention is a practice that simply cannot be automated: the complex context of the workplace environment is what is relevant.

3.3 In data we trust?

When trying to analyse the new phenomenon that is worker surveillance, the analyst keeps coming back to its engine or driving force: data. Worker surveillance is totally reliant on fine-grained personal data and, consequently, on the ability to measure things and to derive actionable conclusions from them. This is a fundamental concern that Sandy J. J. Gould addresses in his chapter in this volume, where he explains that metrics are hard to make and can be noisy, inaccurate and influenced by many factors, resulting in biased, missing information or simply wrong measurement. One example of this is made up of novel safety purposes, such as the monitoring of personal protective equipment compliance through AI, which raise concerns and expose possible limitations such as using an adequate metric, measuring the correct data and having accuracy in pattern recognition and in capturing the essence and subtlety of risk situations (Campero-Jurado et al. 2020).

In short, both data itself and the way it is analysed, which are the core elements of surveillance, should not always be trusted. When worker surveillance takes place, some data is collected through questionable and intrusive means and can be of a highly personal nature. This and other data related to the work environment (temperature, air quality, machine parameters, noise levels, etc), are then analysed using metrics that are unknown to the workforce and which can generate inaccurate results. In other words, surveillance is built on a weak foundation of personal and sensitive data, intrusively collected and potentially inaccurately analysed, and which is hence likely to generate erroneous outcomes (Nath et al. 2017; Gould, this volume).

4. Towards a legal distinction between monitoring and surveillance

Worker surveillance, as described in previous sections, and the imbalance of power and the information it creates in favour of employers needs to be recognised as a self-standing concept in law and legal literature.

As explained in Section 2, employers have always had the ability to monitor workers as a result of an ‘implicit’ or ‘open’ clause in the employment contract. With the possibility of using new, intrusive, invisible and intensive data collection tools, employers can now bring their monitoring power to different levels, thereby establishing a one-sided power relationship with their workers, with little ability for the latter to counterbalance this move given the vast scope of employer oversight and the technical complexities of data science (Sewell and Barker 2001).

The reference to ‘surveillance’ is not casual. The concept, borrowed from sociology, implies a power-centred understanding of the power to monitor (Macnish 2018; Sewell et al. 2012; Marx 2002). Surveillance studies analyse such social interaction independently of legal categories and as a hierarchical structure with two actors: an observer and an observed. In today’s workplace reality, the observer position is further enhanced by third party observers that give even greater monitoring power to the employer. A power-centred understanding of that power in the digital age can help to identify better its new features and actors, and the legal consequences for each of these.

The legal boundaries traditionally imposed on the power to monitor are now being extended in respect of the possibilities of supervision and the culture of the meticulous measurement of workers pushed by the growing market for surveillance technologies (Negrón 2021). The structural difference between traditional worker monitoring and worker surveillance should therefore lead to different legal implications. Worker surveillance has not yet been comprehensively analysed by the ECtHR, which has mainly dealt with traditional monitoring technologies (see Section 2). However, the shaping of such new hierarchies at work systematically presents issues as regards the necessity for these intense and intensive surveillance measures – to be balanced against workers’ fundamental rights such as the right to privacy and data protection.

Currently, there is no case law from the ECtHR addressing data-intensive surveillance at work as such. Yet, the Court has clarified that the ‘necessary’ interference with Article 8 ECHR is a narrowly defined concept: it has none of the flexibility of expressions such as ‘useful’, ‘reasonable’ or ‘desirable’ but implies the existence of a ‘pressing social need’ for the interference in question (*Handyside v United Kingdom*, 1976, para. 48). Thus, interference with Article 8 ECHR must correspond to a pressing social need and, in particular, must remain proportionate to the legitimate aim pursued.

Worker surveillance does not conform to a pressing social need under the ECHR. Thus, it can be described as an unnecessary monitoring power. Most of the new surveillance technology is not strictly necessary to achieve a legitimate employer purpose. Gould shows this point well in his chapter in this volume: 'measuring things about work is difficult, especially work that does not lend itself easily to being broken down into independent atomic parts'; this proves to be particularly relevant in services work in comparison with the manufacturing sector. How could a surveillance provider or an employer prove that looking at the time spent on Facebook, or at the number of times someone looks away from their screen, are representative of productivity or focus?

To prevent such innovations distorting employer authority into something intrusive and unjust, it is essential to ponder carefully the existence of a pressing social need under the ECHR. In several decisions (*Florindo*, 2022; *López Ribalda*, 2019; *Bărbulescu*, 2017), the Court has recognised that significant developments are underway in the field of workforce monitoring. In *Florindo*, the ECtHR in para. 93 explicitly refers to that particular form of surveillance coming under the analysis of the Court for the first time: the data in dispute is not images (see *Köpke*, 2010; *López Ribalda*, 2019; *Antović and Mirković*, 2018), electronic messages (see *Bărbulescu*, 2017) or computer files (see *Libert v. France*, 2018), but geolocation data. According to the Strasbourg judges, this novelty raises a topical question of the type and level of surveillance that is acceptable on the part of an employer with regard to its employees, to be counter-balanced against protection of the private life of employees.

Steering the fast-developing market for surveillance tools makes the so-called suitability (or effectiveness) test as described by Gerards (2013: 473) a topical criterion to be implemented in the Strasbourg Court's forthcoming case law. Any interference with an ECHR fundamental right ought to be realised by means which are effectively capable of realising the aims, or the ends, of the interference. This is a challenging analytical exercise for the Court: factual, statistical or empirical information ought to be scrutinised to ascertain the suitability of the measure. In this regard, Gould (this volume) gives more technical and empirical evidence about the actual usefulness of measurements in the context of worker surveillance. Referring to his arguments shows how easily worker surveillance tools fail the suitability test.

We can, however, already point to the dissenting opinion in *Florindo* where, in para. 17, the dissenting judges explicitly mention that the means of surveillance implemented by the employer (through the GPS) had been erroneously indicated by the majority of the Court as absolutely necessary to achieve the end pursued by the employer (monitoring the use of the company car). The dissenting judges also point out that less intrusive means than GPS were available and, moreover, indicated by Comissão Nacional de Proteção de Dados (CNPD; the Portuguese DPA). In this most recent ECtHR case on worker monitoring, therefore, an explicit reference to a suitability or effectiveness test is already present on the part of the dissenting judges (Molè and Mangan 2023). The GPS was capable of providing more data than necessary, causing an actual surplus of data in the availability of the employer which was not needed to fulfil the purpose of the monitoring.

Via the outcome of this case, it is possible to introduce another test, now urgently needed to filter out unnecessary monitoring power: the least intrusive means test. When evaluating the suitability of the means of surveillance, the Court ought to carry out a factual and empirical assessment of the various means which are contextually available and determine which is the most effective and least intrusive. According to this test, the means to be chosen ought to be the one least harmful from the perspective of the individual rights at stake (Gerards 2013: 481-482). On this point, as explained in Section 3, a general consideration can be drawn. As surveillance is structurally more intrusive than standard monitoring, it is essential that the Court, in future years, undertakes efforts to compare surveillance technologies with others which are less intrusive yet which achieve the same legitimate goal pursued by the employer (for a general discussion on the balancing of ECHR fundamental rights by the ECtHR, see Greer 2004).

5. Conclusion

The power to monitor employees traditionally results from an ‘open term’ in the employment contract that grants employers a set of observational entitlements, in which privacy rights and economic freedoms often collide. This conflict between fundamental rights is being augmented today by new and more intrusive technologies. Hence, differentiating traditional employer monitoring against the background of today’s surveillance technologies highlights the tensions at stake. Borrowing from sociological literature, contemporary monitoring amounts to the surveillance of workers, an activity where the asymmetry of power and information is structurally stronger and based on invisible, intrusive and intensive measurement which is likely to fail a suitability and least intrusive means test under Art. 8 ECHR. Worker surveillance shows features of a disproportionate and unlawful power, predicated on the belief that anything and everything that is measurable should be measured. The interconnectedness and natural nexus between autonomy and privacy (Hendrickx 2018) is broken. Human dignity itself is at stake since, as law professor Nita Farahany says ‘there is no existing set of legal rights that protects us from employers scanning the brain or hacking the brain’ (Dockser Marcus 2023).

ECtHR case law has been referenced in support of this line of argument with the aim of identifying the legal boundary beyond which worker monitoring becomes illegitimate worker surveillance. Here, a more favourable interpretation of Article 8 ECHR for workers might be suggested. Pointing to surveillance as a self-standing legal concept helps to tame some of the substantial risks of unnecessary and systematic monitoring under which worker autonomy is eroded, the principle of prevention in OSH is abandoned in favour of ‘automated prevention’ and fundamental rights are violated. All of this is fuelled by personal and sensitive data that is collected intrusively, yet this may be being inaccurately measured. The necessity and proportionality tests should become a legal obligation when introducing worker monitoring technologies. Action is urgently needed not just to regulate or set limits on surveillance, but to define it legally as a prohibited practice which conflicts with the most essential fundamental rights at work.

References

Adams-Prassl J. (2019) What if your boss was an algorithm? Economic incentives, legal challenges, and the rise of artificial intelligence at work, Comparative Labor Law and Policy Journal, 41 (1), 123.

AI Now Institute (2023) Algorithmic management: Restraining workplace surveillance, 11 April 2023. https://ainowinstitute.org/publication/algorithmic-management

Al Jassmi H., Ahmed S., Philip B., Al Mughairbi F. and Al Ahmad M. (2019) E-happiness physiological indicators of construction workers’ productivity: A machine learning approach, Journal of Asian Architecture and Building Engineering, 18 (6), 517–526. https://doi.org/10.1080/13467581.2019.1687090

Agosti C., Bronowicka J., Polidoro A. and Priori G. (2023) Exercising workers’ rights in algorithmic management systems: Lessons learned from the Glovo-Foodinho digital labour platform case, Report 2023.11, ETUI. https://www.etui.org/publications/exercising-workers-rights-algorithmic-management-systems

Aloisi A. and De Stefano V. (2022) Essential jobs, remote work and digital surveillance: Addressing the COVID‐19 pandemic panopticon, International Labour Review, 161 (2), 289–314. https://doi.org/10.1111/ilr.12219

Badri A., Boudreau-Trudel B. and Souissi A.S. (2018) Occupational health and safety in the industry 4.0 era: A cause for major concern?, Safety Science, 109, 403–411. https://doi.org/10.1016/j.ssci.2018.06.012

Baiocco S., Fernández Macías E., Rani U. and Pesole A. (2022) The algorithmic management of work and its implications in different contexts, JRC Working Papers Series on Labour, Education and Technology 2022/02, European Commission. https://joint-research-centre.ec.europa.eu/publications/algorithmic-management-work-and-its-implications-different-contexts_en

Bales R.A. and Stone K.V. (2020) The invisible web at work: Artificial intelligence and electronic surveillance in the workplace, Berkeley Journal of Employment and Labor Law, 41 (1). https://doi.org/10.15779/Z380000085

Ball K. (2010) Workplace surveillance: An overview, Labor History, 51 (1), 87–106. https://doi.org/10.1080/00236561003654776

Benlian A. et al. (2022) Algorithmic management: Bright and dark sides, practical implications, and research opportunities, Business and Information Systems Engineering, 64 (6), 825–839. https://doi.org/10.1007/s12599-022-00764-w

Borle P., Reichel K., Niebuhr F. and Voelter-Mahlknecht S. (2021) How are techno-stressors associated with mental health and work outcomes? A systematic review of occupational exposure to information and communication technologies within the technostress model, International Journal of Environmental Research and Public Health, 18 (16), 8673. https://doi.org/10.3390/ijerph18168673

Burnett J.R. and Lisk T.C. (2021) The future of employee engagement: Real-time monitoring and digital tools for engaging a workforce, in Segalla M. (ed.) International perspectives on employee engagement, Routledge, 117–128.

Brynjolfsson E., Li D. and Raymond L.R. (2023) Generative AI at work, Working Paper 31161, National Bureau of Economic Research. https://doi.org/10.3386/w31161

Cabrelli D. and Graveling R. (2019) Health and safety in the workplace of the future, European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/638434/IPOL_BRI(2019)638434_EN.pdf

Campero-Jurado I., Márquez-Sánchez S., Quintanar-Gómez J., Rodríguez S. and Corchado J.M. (2020) Smart helmet 5.0 for industrial Internet of things using artificial intelligence, Sensors, 20 (21). https://doi.org/10.3390/s20216241

Carby-Hall J. (2003) The contractual nature of social law, Managerial Law, 45 (3/4), 23–107. https://doi.org/10.1108/03090550310770893

Castro I. and Ramos D.G. (2017) Understanding the management of occupational health and safety risks through the consultation of workers, in Arezes P.M. et al. (eds.) Occupational safety and hygiene V, CRC Press, 29–34.

Chan N.K. (2019) The rating game: The discipline of Uber's user-generated ratings, Surveillance and Society, 17 (1/2), 183–190. https://doi.org/10.24908/ss.v17i1/2.12911

Cheng B., Fan C., Fu H., Huang J., Chen H. and Luo X. (2022) Measuring and computing cognitive statuses of construction workers based on electroencephalogram: A critical review, IEEE Transactions on Computational Social Systems, 9 (6), 1644–1659. https://doi.org/10.1109/TCSS.2022.3158585

Coase R.H. (1937) The nature of the firm, Economica, 4 (16), 386–405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

De Cremer D. and Stollberger J. (2022) Are people analytics dehumanizing your employees?, Harvard Business Review. https://hbr.org/2022/06/are-people-analytics-dehumanizing-your-employees

Dockser Marcus A. (2023) When your boss is tracking your brain, The Wall Street Journal, 15 February 2023. https://www.wsj.com/articles/brain-wave-tracking-privacy-b1bac329?mkt_tok=MTM4LUVaTS0wNDIAAAGJ_MWOqN2F8QfijbjrPEKP26_kBSJFTuoGXkacR02Cb7SKzIMT5hUfJrZaL1cQ51GnM7DlnL8ifJxaQGhubGvH4Hw4djn-dcXaLjaKnOHE10ki

EDPS (2019) Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, European Data Protection Supervisor. https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

EU-OSHA (2007) Factsheet 80 — Risk assessment — roles and responsibilities. https://osha.europa.eu/en/publications/factsheet-80-risk-assessment-roles-and-responsibilities

EU-OSHA (2023) Using AI for task automation while protecting workers: Eight case studies provide new insights. https://osha.europa.eu/en/highlights/using-ai-task-automation-while-protecting-workers-eight-case-studies-provide-new-insights

European Commission (2021) Proposal for a Directive of the European Parliament and the council on improving working conditions in platform work, COM(2021) 762 final, 9.12.2021. https://eures.ec.europa.eu/eu-proposes-directive-protect-rights-platform-workers-2022-03-17_en

European Data Protection Board (2020a) Hamburg commissioner fines H&M 35.3 million euro for data protection violations in service centre. https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en

European Data Protection Board (2020b) State commissioner for data protection in lower Saxony imposes € 10.4 million fine against notebooksbilliger.de. https://edpb.europa.eu/

news/national-news/2021/state-commissioner-data-protection-lower-saxony-imposes-eu-104-million-fine_en

European Social Partners (2020) European social partners framework agreement on digitalisation, ETUC. https://www.etuc.org/system/files/document/file2020-06/Final%20 22%2006%2020_Agreement%20on%20Digitalisation%202020.pdf

Farahany N.A. (2023) The battle for your brain: Defending the right to think freely in the age of neurotechnology, St. Martin's Press.

Frick K. (2011) Worker influence on voluntary OHS management systems - A review of its ends and means, Safety Science, 49 (7), 974–987. https://doi.org/10.1016/j.ssci.2011.04.007

Gallup (2023) Gallup's employee engagement survey: Ask the right questions with the Q12® survey. https://www.gallup.com/workplace/356063/gallup-q12-employee-engagement-survey.aspx

Gerards J. (2013) How to improve the necessity test of the European Court of Human Rights. International Journal of Constitutional Law, 11 (2), 466–490. https://doi.org/10.1093/icon/mot004

GPDP (2021) Riders: Italian SA says no to algorithms causing discrimination. A platform in the Glovo group fined EUR 2.6 million, Garante per la Protezione dei Dati Personali https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677377#english

Greer S. (2004) 'Balancing' and the European Court of Human Rights: A contribution to the Habermas-Alexy debate, The Cambridge Law Journal, 63 (2), 412–434. https://doi.org/10.1017/S0008197304006634

Hendrickx F. (2018) From digits to robots: the privacy-autonomy nexus in new labor law machinery, Comparative Labor Law and Policy Journal, 40 (3), 365–388.

Hildebrandt M. (2022) The issue of proxies and choice architectures. Why EU law matters for recommender systems, Frontiers in Artificial Intelligence, 5. https://doi.org/10.3389/frai.2022.789076

Hildebrandt M. (2023) Sustainable software: Issues of bias, proxies and ground truthing in machine learning. https://www.cohubicol.com/assets/uploads/hildebrandt-api-keynote.pdf

ICO (2022) Employment practices: Monitoring at work draft guidance, Information Commissioner's Office. https://ico.org.uk/media/about-the-ico/consultations/4021868/draft-monitoring-at-work-20221011.pdf

Jebelli H., Choi B. and Lee S. (2019) Application of wearable biosensors to construction sites. I: Assessing workers' stress, Journal of Construction Engineering and Management, 145 (12), 04019079. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001729

Laker B., Godley W., Patel C. and Cobb D. (2020) How to monitor remote workers—Ethically, MIT Sloan Management Review. https://sloanreview.mit.edu/article/how-to-monitor-remote-workers-ethically/

Lupton D. (2016) The quantified self: A sociology of self-tracking, Polity.

Macnish K. (2018) The ethics of surveillance: An introduction, Routledge.

Malik A. (2023) Artificial intelligence in health and safety, SafetyPedia. https://safetypedia.com/safety/artificial-intelligence-in-health-and-safety/

Mangan D. (2022) From monitoring of the workplace to surveillance of the workforce, in Gyulavári T. and Menegatti E. (eds.) Decent work in the digital age: European and comparative perspectives, Bloomsbury, 311–329.

Marx G.T. (2002) What's new about the 'new surveillance'? Classifying for change and continuity, Surveillance and Society, 1 (1), 9–29. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Marx G.T. (2015) Surveillance studies, International Encyclopedia of the Social and Behavioral Sciences, 733–741. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Menéndez M., Benach J. and Vogel L. (2009) The impact of safety representatives on occupational health: A European perspective, Report 107, ETUI.

Molè M. (2022) The Internet of things and artificial intelligence as workplace supervisors: Explaining and understanding the new surveillance to employees beyond art. 8 ECHR, Italian Labour Law E-Journal, 15 (2), 87–103. https://doi.org/10.6092/ISSN.1561-8048/15598

Molè M. and Mangan D. (2023) 'Just more surveillance': The ECtHR and workplace monitoring, European Labour Law Journal, 14 (4), 694–700. https://doi.org/10.1177/20319525231201274

Moore P.V. (2018) Tracking affective labour for agility in the quantified workplace, Body and Society, 24 (3), 39–67. https://doi.org/10.1177/1357034X18775203

Nath N.D., Akhavian R. and Behzadan A.H. (2017) Ergonomic analysis of construction worker's body postures using wearable mobile sensors, Applied Ergonomics, 62, 107–117. https://doi.org/10.1016/j.apergo.2017.02.007

Negrón W. (2021) Little tech is coming for workers. A framework for reclaiming and building worker power, Coworker.org. https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf

Nielsen K.J. (2014) Improving safety culture through the health and safety organization: A case study, Journal of Safety Research, 48, 7–17. https://doi.org/10.1016/j.jsr.2013.10.003

Ollé-Espluga L., Vergara-Duarte M., Belvis F., Menéndez-Fuster M., Jódar P. and Benach J. (2015) What is the impact on occupational health and safety when workers know they have safety representatives?, Safety Science, 74, 55–58. https://doi.org/10.1016/j.ssci.2014.11.022

Ponce del Castillo A. (2020) COVID-19 contact-tracing apps: How to prevent privacy from becoming the next victim, Policy Brief 5/2020, ETUI. https://www.etui.org/publications/policy-briefs/european-economic-employment-and-social-policy/covid-19-contact-tracing-apps-how-to-prevent-privacy-from-becoming-the-next-victim .

Reiman A., Kaivo-Oja J., Parviainen E., Takala E.-P. and Lauraeus T. (2021) Human factors and ergonomics in manufacturing in the industry 4.0 context–A scoping review, Technology in Society, 65, 101572. https://doi.org/10.1016/j.techsoc.2021.101572

Riso S. (2020) Employee monitoring and surveillance: The challenges of digitalisation, Publications Office of the European Union. https://www.eurofound.europa.eu/en/publications/2020/employee-monitoring-and-surveillance-challenges-digitalisation

Rogers B. (2023) Workplace data is a tool of class warfare, Boston Review. https://www.bostonreview.net/articles/workplace-data-is-a-tool-of-class-warfare/

Schulte P.A. et al. (2020) Potential scenarios and hazards in the work of the future: A systematic review of the peer-reviewed and gray literatures, Annals of Work Exposures and Health, 64 (8), 786–816. https://doi.org/10.1093/annweh/wxaa051

Sewell G. and Barker J.R. (2001) Neither good, nor bad, but dangerous: Surveillance as an ethical paradox, Ethics and Information Technology, 3 (3), 181–194. https://doi.org/10.1023/A:1012231730405

Sewell G., Barker J.R. and Nyberg D. (2012) Working under intensive surveillance: When does 'measuring everything that moves' become intolerable?, Human Relations, 65 (2), 189–215. https://doi.org/10.1177/0018726711428958

Stark D. and Pais I. (2020) Algorithmic management in the platform economy, Sociologica, 14 (3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

Swan M. (2013) The quantified self: Fundamental disruption in big data science and biological discovery, Big Data, 1 (2), 85–99. https://doi.org/10.1089/big.2012.0002 van Rijmenam M. (2023) The transformative role of AI in revolutionising workplace health and safety, The Digital Speaker, 3 August 2023. https://www.thedigitalspeaker.com/transformative-role-ai-revolutionising-workplace-health-safety/#:~:text=Predictive%20modelling%20uses%20sophisticated%20algorithms,measures%20and%20protect%20their%20workforce

Vitard A. (2023) Amazon risque une amende de 170 millions d'euros pour sa gestion des données de productivité des salariés, L'Usine Digitale, 18 Sptember 2023. https://www.usine-digitale.fr/article/amazon-risque-une-amende-de-170-millions-d-euros-pour-sa-gestion-des-donnees-de-productivite-des-salaries.N2171902

Wadsworth E. and Walters D. (2019) Safety and health at the heart of the future of work: Building on 100 years of experience, ILO. https://www.ilo.org/safework/events/safeday/WCMS_687610/lang--en/index.htm

Wang D., Chen J., ZhaoD., Dai F., Zheng C. and Wu X. (2017) Monitoring workers' attention and vigilance in construction activities through a wireless and wearable electroencephalography system, Automation in Construction, 82, 122–137. https://doi.org/10.1016/j.autcon.2017.02.001

Zuboff S. (2019) The age of surveillance capitalism: The fight for a human future at the new frontier of power, PublicAffairs.

Case law

— *Antović and Mirković v. Montenegro* (European Court of Human Rights 28 February 2018). https://hudoc.echr.coe.int/fre?i=001-178904
— Article 29 Data Protection Working Party (2017). Opinion 2/2017 on Data Processing at Work
— *Bărbulescu v. Romania*, Application no. 61496/08 (European Court of Human Rights 2017). https://hudoc.echr.coe.int/fre?i=001-177082
— *Copland v. United Kingdom* (European Court of Human Rights 3 April 2007).
— *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* (European Court of Human Rights 13 December 2022). https://hudoc.echr.coe.int/fre?i=002-13935
— *Halford v. UK* (European Court of Human Rights 25 June 1997).
— *Handyside v United Kingdom*, 5493/72 (European Court of Human Rights 1976).
— *Köpke v. Germany* (European Court of Human Rights 5 October 2010).
— *Libert v. France* (European Court of Human Rights 22 February 2018). https://hudoc.echr.coe.int/rus/#{%22itemid%22:[%22001-181273%22]}
— *López Ribalda and Others v. Spain* (European Court of Human Rights 17 October 2019). https://hudoc.echr.coe.int/fre?i=002-12630

All links were checked on 14.02.2024.

Cite this chapter: Ponce Del Castillo A. and Molè M. (2024) Worker monitoring vs worker surveillance: the need for a legal differentiation, in Ponce del Castillo (ed.) Artificial intelligence, labour and society, ETUI.