RESEARCH REPORT

Eurofound

Working conditions

Employee monitoring and surveillance: The challenges of digitalisation

Employee monitoring and surveillance: The challenges of digitalisation

Eurofound

European Foundation for the Improvement of Living and Working Conditions

When citing this report, please use the following wording:
Eurofound (2020), *Employee monitoring and surveillance: The challenges of digitalisation*, Publications Office of the European Union, Luxembourg.

Author: Sara Riso (Eurofound)

Research managers: Agnès Parent-Thirion and David Foden (Eurofound)

Research project: Timely information for EurWORK – topical updates (190302)

Provider: The Network of Eurofound Correspondents provided input for this report

Acknowledgements: The author would like to thank Eurofound colleagues (David Foden, Irene Mandl and Agnès Parent-Thirion) who reviewed this topical update and provided comments and suggestions.

Luxembourg: Publication Office of the European Union

Print:	ISBN 978-92-897-2124-0	doi:10.2806/228154	TJ-01-20-638-EN-C
PDF:	ISBN 978-92-897-2123-3	doi:10.2806/424580	TJ-01-20-638-EN-N

This report and any associated materials are available online at http://eurofound.link/ef2008

Research carried out prior to the UK's withdrawal from the European Union on 31 January 2020, and published subsequently, may include data relating to the 28 EU Member States. Following this date, research only takes into account the 27 EU Member States (EU28 minus the UK), unless specified otherwise.

This report presents the results of research conducted largely prior to the outbreak of COVID-19 in Europe in February 2020. For this reason, the results do not fully take account of the outbreak.

The European Foundation for the Improvement of Living and Working Conditions (Eurofound) is a tripartite European Union Agency established in 1975. Its role is to provide knowledge in the area of social, employment and work-related policies according to Regulation (EU) 2019/127.

European Foundation for the Improvement of Living and Working Conditions

Telephone: (+353 1) 204 31 00
Email: information@eurofound.europa.eu
Web: www.eurofound.europa.eu

Contents

List of abbreviations

AI	artificial intelligence
BusinessEurope	Confederation of European Business
CCTV	closed-circuit television
ECS	European Company Survey
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
ETUC	European Trade Union Confederation
ETUI	European Trade Union Institute
FRA	Fundamental Rights Agency
GDPR	General Data Protection Regulation
GPS	global positioning system
ICT	information and communications technology
ILO	International Labour Organization
IoT	internet of things
OECD	Organisation for Economic Co-operation and Development
RFID	radio-frequency identification
SMEUnited	Association of Crafts and SMEs in Europe
SMEs	small and medium-sized enterprises

Introduction

Background and scope of the report

Employee monitoring and surveillance are not new phenomena. To varying extents, employers routinely engage in the monitoring of employees' activities. There are legitimate grounds for doing so: for example, to protect an organisation's assets and property rights, track performance and optimise processes, ensure occupational safety and compliance with legal and regulatory requirements, and prevent criminal or fraudulent activities. In some sectors, there may be a legal or regulatory requirement for employers to carry out a certain degree of monitoring. With remote working becoming more common, employers may view the use of some monitoring systems as legitimate – to ensure accountability owing to the flexibility that such working arrangements entail. Remote working – and with it a perceived need to monitor performance and check on employees – continues to be the default mode of operation in traditionally mobile occupations: for example, salespeople who are required to travel extensively for work purposes.

Although employee monitoring and surveillance involve similar management practices, there are important differences to bear in mind. While employee monitoring is generally confined to capturing work-related activities, surveillance is more intrusive, as it employs technologies that cover a broader range of information (on both work- and non-work-related activities) (McNall and Stanton, 2011). While there are overlaps between monitoring and surveillance practices, the distinction between them suggests that greater ethical and privacy concerns arise from employee surveillance. Surveillance has a more negative connotation in the public discourse than monitoring. Subjects who are aware that they are under surveillance most or all of the time are bound to adjust their behaviour accordingly, suggesting that surveillance violates an individual's autonomy in a way that is often associated with dystopian characteristics (Torpey, 2007; Ball, 2010; Zuboff, 2019).

Technological advances have certainly expanded employee monitoring and surveillance capabilities, but the concept of employee monitoring and surveillance is an old one. At their core, employee monitoring and surveillance encompass the basic tenets of Taylorism, which originated in the time and motion studies used in early 'scientific management' practice research. These studies entailed continuous observation of workers and recording the time taken to accomplish work tasks with a view to improving workers' efficiency and productivity (Jeske and Kapasi, 2017). Although Taylorism is considered outdated nowadays, the pervasiveness and ubiquity of new digital technologies in the workplace has given rise to a modern version of scientific management known as 'digital Taylorism' or 'new Taylorism' (Owczarek and Chełstowska, 2016).

Both European and national legislators are increasingly confronted with new and ever-evolving sets of issues arising from technological change in the area of employee monitoring and surveillance. As new digital technologies are moving targets, regulatory provisions in EU Member States are often out of step with technological developments. Technological change has opened the door to more intrusive employee monitoring and surveillance – going beyond the use of conventional forms of monitoring, such as closed-circuit television (CCTV) cameras and the monitoring of emails, internet usage and telephone calls. Digital technologies are increasingly ubiquitous and allow for connectivity anytime and anywhere. A case in point are location-sensing technologies relying on global positioning system (GPS) or radio-frequency identification (RFID) devices, which can be used to provide always-on and real-time location tracking of the whereabouts of employees. While these technologies can help to ensure compliance with policies on rest breaks and the traceability of company assets and resources, they can also contribute to increasing work intensity, reducing idle time and sanctioning underperformance. These issues are likely to become more prominent as technologies – such as wearable and biometric technologies – quickly develop and become more sophisticated and increasingly affordable, enabling increasingly powerful and intrusive employee monitoring.

New digital technologies can harness many benefits and opportunities in the labour market and in terms of working conditions; recently, they have made it possible for many people to work from home during the COVID-19 pandemic. However, they have also opened up new opportunities to monitor workers by means of software that can log keystrokes, track (mouse) movements, take webcam shots of employees in front of their computers, and measure the quality of the air in workplaces and the performance of (industrial) machines. These technologies can be used in a positive way to monitor individual exposure to dangerous substances to limit the risks of people working in isolation. With the increasing use of devices endowed with sensors that capture every piece of information available about the surrounding environment, new types of employee data can be collected (and data can be collected at a greater level of granularity and scale than ever before) – whether employees are working remotely or in the workplace. Advances in data analytics also make it possible to generate inferences from the data collected and even predict employees' future behaviour.

In the context of the increasing digitalisation of work, there are many issues related to employee monitoring that warrant the attention of policymakers. As well as the often-cited privacy and ethical concerns, there are also important implications for worker–employer relations, as digitally enabled monitoring and surveillance

inevitably shift power dynamics in the workplace. In addition, empirical analysis on the use of teleworking and information and communications technology (ICT) mobile work shows that remote working can have both positive and negative characteristics from a job quality perspective, depending on the individual, the company and the type of job (Eurofound, 2020d). For example, remote working may result in irregular working hours and employees may use work devices for both personal and work reasons, blurring the boundaries between work and private life while providing greater autonomy for workers to organise their working time (Sostero et al, 2020).

Digitally enabled employee monitoring can also contribute to the gamification of work, making workers feel that they are constantly in competition with one another. This prevents them from teaming up and possibly leads to workers having reduced organising and negotiating power. There are also wide-ranging implications for job quality, as the side-effects of constant and pervasive employee monitoring include reduced work autonomy, greater work intensification, higher levels of stress and anxiety, a diminished level of trust towards management and greater interference of work in the private sphere, to mention just a few. Technologies used for employee monitoring could, however, be deployed to benign effect by responsible employers for the benefit of employees. For example, wearable devices may be used to augment human capabilities, overcome physical limitations and increase safety, especially in hazardous or emergency situations. They can also guide employees in performing their tasks more effectively and provide them with useful information about their work environment.

Against this background, the objectives of this report are threefold:

- to map regulatory approaches to employee monitoring and surveillance in the 27 EU Member States, Norway and the United Kingdom (UK), regulatory compliance and case law, and the positions and views of policy stakeholders (Chapter 1)
- to give an overview of new forms of employee monitoring, complemented by empirical evidence on the extent of employee monitoring in EU Member States and the UK (Chapter 2)
- to review recent research on the implications of employee monitoring and surveillance for job quality (Chapter 3).

This report explores employee monitoring and surveillance only in relation to dependent employment. Outside the scope of this review are employee monitoring practices used in the context of self-employment, freelancing and some new forms of employment in which the employment status is unclear (as in the case of platform work).

The information and data used for this report are drawn from a mix of sources. These include information provided in late 2019 by the Network of Eurofound Correspondents on the basis of a semi-standardised questionnaire. This information is supplemented by desk research and an analysis of data from the 2019 European Company Survey (ECS) carried out jointly by Eurofound and Cedefop, which explored the extent of employee monitoring in establishments in the EU and the UK and pointed to some of the implications for work organisation (Eurofound, 2020a).

Defining digital technologies

A number of technologies can be used for employee monitoring and surveillance. To guide the reader, Table 1 provides definitions of the technologies mentioned most frequently throughout the report (the list is not exhaustive). The definitions draw on previous Eurofound research (Eurofound, 2018, 2020b) and on European and national sources.

Table 1: Definitions of technologies used for employee monitoring and surveillance

Technology	Definition
Artificial intelligence (AI)	AI is a general-purpose technology that enables and supports the application of many other technologies (Brynjolfsson et al, 2017). AI covers automated and semi-automated systems, including algorithmic decision-making and management. The definition adopted by the European Commission refers to narrow AI, which uses machine learning and deep learning tools to extract information from an enormous number of data and to generate new value based on models built with those data (Eurofound, 2020b).
Big data and data analytics	According to the definition provided by the European Commission (2020b): *Big data refers to large amounts of data produced very quickly by a high number of diverse sources. Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, GPS signals, etc.* 'Data analytics' refers to the use of digital tools for analysing data collected at the establishment or from other sources (Eurofound, 2020a).
Biometrics	According to the European Commission (2018), 'biometric technologies refer to all processes used to recognize, authenticate and identify persons based on physical and/or behavioural characteristics'. In a similar vein, the French Data Protection Authority defines 'biometrics' as 'all automated processes used to recognise an individual by quantifying their physical, physiological or behavioural characteristics (fingerprints, blood vessel patterns, iris structure, etc.)' (CNIL, 2019).
Global positioning system (GPS)	GPS is a global navigation satellite system whereby data are transmitted from satellites in space to earth-bound receivers to notify them of their location. GPS can localise and trace goods and people when used in combination with mobile systems such as geography information systems and advanced internet applications (Kanngieser, 2013).
Internet of things (IoT) and 'wearables'	The IoT is made up of networked sensors attached to outputs, inputs, components, materials or tools used in production. Such sensors create a cyber-physical system in which the information collected is fed, via the internet, to computers to gather data about production and work processes and to analyse these data with unprecedented granularity. Wearables are devices comprising electronics, software and sensors that are designed to be worn on the body (Billinghurst and Starner, 1999). Examples include smartwatches, head-mounted displays, body cameras and smart clothing.
Radio-frequency identification (RFID)	RFID is a system of electronic tagging used to identify and trace objects and people and store information. There are three components: the microchip tag, the receiver and the back-end database to manage the data from the tag (Kanngieser, 2013).

1 Regulatory approaches in Europe

Background and issues at stake

Employee monitoring is not addressed explicitly in EU legislation, but privacy and data protection rights that may be impinged upon by employee monitoring are. The most important piece of EU legislation in this regard is the General Data Protection Regulation (Regulation (EU) 2016/679), replacing Directive 95/46/EC – known as the GDPR. Entering into force in May 2018 and applicable in all EU Member States, the GDPR regulates the collection, use and transfer of personal data and sets out provisions that apply to all data-processing operations, including employee monitoring. The prior informed consent of the employee is, for example, required for the introduction of employee monitoring. However, it is in the remit of individual Member States to introduce specific provisions with regard to the processing of employee data for a variety of purposes, from recruitment to health and safety:

> *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, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*
>
> (GDPR, Article 88(1))

According to the European Fundamental Rights Agency (FRA), the GDPR has modernised the pre-existing EU data protection legislation so that it meets the new privacy challenges posed by the development of digital technologies. With regard to employment data, FRA questions, however, the validity of consent as a legal basis for processing data about employees in view of 'the economic imbalance between employer and employees' (FRA and Council of Europe, 2018, p. 330). In the same spirit, the Article 29 Working Party (WP 29) stated that 'employees are seldom in a position to freely give, refuse or revoke consent' (WP 29, 2017).[1] This is reflected in the guidelines of the European Data Protection Board (EDPB) on consent adopted in 2020:

> *The EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee … Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.*
>
> (EDPB, 2020, p. 9)

Another issue raised by FRA concerns the extent of data collected about employees, especially in the context of greater connectivity of internet of things (IoT)-enabled devices and enhanced processing capabilities, which make the issue of informed consent even more challenging. Individuals often lack a clear understanding of the extent of the data collected, of the technical functioning of the processing and therefore of what they are consenting to. National data protection authorities have so far taken the view that big data falls within the scope of data protection law and so must comply with the data protection legislation.

Before the GDPR entered into force, WP 29 warned against the implications of digital technologies for workers' rights:

> *If there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring.*
>
> (WP 29, 2017, p. 9)

Furthermore, WP 29 highlighted some risks associated with the use of technologies to monitor communication in the workplace, which can have 'a chilling effect on the fundamental rights of employees to organise, set up workers' meetings, and to communicate confidentially' (WP 29, 2017, p. 9).

If misused, digital technologies can present a serious threat to workers' freedom of association and potentially weaken workers' negotiating powers. The rights to freedom of association and collective bargaining are expressed in the International Bill of Human Rights and the International Labour Organization's (ILO's) Declaration on Fundamental Principles and Rights at Work (ILO, undated). The ILO's code of practice (ILO, 1997) on the protection of workers' personal data also sets out key principles in employee monitoring, including workers' right to be informed of the use of technologies at the workplace and the requirement for employers to consider any potential consequences for and infringement of workers' individual and collective rights.

WP 29 also noted the following:

> *Owing to the capabilities of such technologies, employees may not be aware of what personal data are*

1 The WP 29 was an independent European working party that served as an advisory body dealing with issues relating to the protection of privacy and personal data until 25 May 2018. It has been replaced by the European Data Protection Board under the new GDPR.

> *being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself.*
>
> (WP 29, 2017, p. 10)

The same, if not greater, risks arise from the use of intrusive digital technologies to track employees' locations, movements and behaviour.

During the legislation process for the GDPR, WP 29 raised concerns in relation to the use of automated processing and 'profiling', which refers to algorithmic inference drawn from personal data.[2] This specific aspect had been subject to intense legislative debate prior to the adoption of the GDPR and concluded with a provision (GDPR, Article 22) that precludes 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.

While some experts view this provision as 'forward-looking' (Aloisi and Gramano, 2019), for others it is open to interpretation and is not clear (IAPP, 2016). Concerns have also been raised by some scholars, who argue that the GDPR does not address the new risks posed by inferential analytics (Wachter and Mittelstadt, 2019). In the employment context, advanced big-data analytics can be used to draw inferences and predictions about employees' behaviour from the data collected, based on which employers may make important decisions. However, these decisions may be unfair or discriminatory vis-à-vis the employees, as they are taking so-called 'human standards' out of the equation.[3] According to legal experts, the limited emphasis in the GDPR's provisions on the risks connected to the use of big data and its processing partly reflects a certain ambivalence in EU policymaking when it comes to new digital technologies and big data in particular (IAPP, 2016). In the European Commission's digital single market strategy, big data, AI and other new digital technologies are viewed as sources of innovation and of strategic importance for EU competitiveness. There is, nonetheless, an awareness of the challenges posed by these new technologies, particularly so-called 'high-risk' AI systems (for example, those used for recruitment processes). The recent communication setting out *A European strategy for data* (European Commission, 2020a) and the white paper *On artificial intelligence – A European approach to excellence and trust* (European Commission, 2020c) propose a regulatory approach for these high-risk AI systems, advocating strict rules and a more flexible framework for less risky systems.

While the Confederation of European Business (BusinessEurope, 2020a) has emphasised the need to 'get the balance between open innovation and societal protection correct', both the European Trade Union Confederation (ETUC, 2020) and UNI Europa (2020) recommend a greater focus on social dialogue. The European Trade Union Institute (ETUI), the ETUC's research institute, has reiterated this appeal and called for the development of a governance framework in relation to the use of AI (along with other new technologies), with the broad participation of the social partners. The aim of this framework is to preserve workers' fundamental rights and conditions, and ultimately ensure that the EU remains 'faithful to its democratic identity' (ETUI, 2020).

With the use of digital technologies in the workplace becoming increasingly pervasive, the responsibilities of the employer are likely to undergo some change. An important area affected by technological change in the workplace is occupational health and safety. The EU Framework Directive for occupational safety and health (Directive 89/391/EEC) lays down general principles and obligations concerning the prevention of occupational risks and the protection of the safety and health of workers. The directive does not, however, explicitly address the new challenges posed by digital technologies – including surveillance technologies – or the emergence of new types of health problems and risks that such technologies can generate (European Parliament, 2019).

Another source of concern is neurosurveillance at work. There are calls for the recognition of new human rights – including rights to mental privacy and integrity – in the face of developments in neurotechnology (Ienca and Andorno, 2017). In this regard, the Organisation for Economic Co-operation and Development (OECD) adopted, in 2019, the first international legal instrument on neurotechnology, defining personal brain data as 'data relating to the functioning or structure of the human brain of an identified or identifiable individual that includes unique information about their physiology, health, or mental states' (OECD, 2019). The OECD (2019) recommends the promotion of policies that 'protect personal brain data from being used to discriminate against or to inappropriately exclude certain persons or populations, especially for commercial purposes or in the context of legal processes, employment, or insurance'.

National regulatory frameworks

General and new regulatory approaches

Most Member States' legislation follows a technologically neutral approach, setting general rules of wide applicability that, at least in principle, cover all types of monitoring and processing. The GDPR has been drafted with the intention of covering technological developments, specifically referring to the fact that 'the scale of the collection and sharing of personal data has increased significantly' and that 'technology allows … use of personal data on an unprecedented scale' (GDPR, recital 6).

2 Article 4(4) of the GDPR defines profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

3 'Human standards' are promoted by the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA) as part of its global initiative on the ethics of autonomous and intelligent systems.

One specific area that is addressed – and to some extent regulated – in several countries is the use of intrusive digital technologies such as GPS tracking and biometrics (hand readers, fingerprint readers or face recognition devices). For example, the recently amended French Data Protection Act (law 2018-493 of 20 June 2018) regulates some forms of employee monitoring, including those using more advanced digital technologies. According to the provisions, biometric access-control devices must comply with a so-called 'model regulation' drawn up by the French Data Protection Authority (CNIL). For example, employers must justify and document their choice of a biometric device and explain why the use of other, more standard, measures (for example, badges and passwords) is not sufficient given the level of security required.

In addition, the new Portuguese Data Protection Act (law 58 of 8 August 2019) has specific provisions about the processing of biometric data in the workplace and states that the processing of employees' biometric data is permitted only for the purpose of monitoring attendance and controlling access to the employer's premises. Furthermore, the Portuguese Labour Code (law 7 of 12 February 2009) stipulates that the employer may use remote monitoring mechanisms in the workplace by way of technological equipment only for the purpose of protecting workers, clients and property – and not for monitoring employees' performance.

A novel regulatory approach has been introduced in Spain, with Organic Law 3/2018 on the protection of personal data and guaranteeing digital rights, which introduces the new concept of 'digital rights', setting limits on the use of digitally enabled monitoring. This law recognises the right of employees to privacy in the use of digital devices provided by their employer and stipulates that employers must establish criteria for the use of digital devices for employee monitoring in compliance with the law. The digital rights referred to include the right to disconnect and the rights of employees to rest, leave, holidays, personal privacy and family privacy. The law leaves the implementation of the right to disconnect and additional guarantees in relation to processing the personal data of workers and the protection of digital rights to the collective bargaining parties at sector or company level. As well as in Spain, the right to disconnect is also included in legislation in Belgium, France and Italy and is currently being discussed by policy stakeholders in a number of other countries (Eurofound, 2020c). However, it should be noted that, as of December 2019, no specific provisions were found in the available national legislation on the right to disconnect in relation to the use of new digital technologies for the monitoring of remote workers.

Table 2 provides an overview of the most relevant national legislation addressing employee monitoring and surveillance.

Table 2: Relevant national legislation addressing employee monitoring and surveillance

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Austria	Austrian Labour Constitution Act and Austrian Data Protection Act	Very broad definition covering mechanical control, control using monitoring technologies and control by other people. Co-determination and participation of the works council is mandatory if the employer wishes to introduce employee monitoring that is deemed to affect human dignity.	Temporary screening of and access to content on a computer (for example, work emails) and GPS tracking are subject to co-determination. Video monitoring for the purpose of monitoring performance is prohibited.
Belgium	Article 8 of the European Convention on Human Rights and Article 22 of the Belgian Constitution assert the right to privacy of employees. Collective agreements regulate specific forms of monitoring (for example, collective agreement No. 68 of 16 June 1998 on the use of camera surveillance at the workplace and collective agreement No. 81 of 26 April 2002 on electronic monitoring of internet and emails).	The principles of legality, legitimacy and proportionality apply.	Monitoring of electronic communications is permitted only for the purposes listed in collective agreement No. 81. Camera surveillance at the workplace is permitted only for the objectives stipulated in collective agreement No. 68. GPS tracking must be justified. Employees must be informed beforehand about the existence, purpose and duration of the monitoring.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Bulgaria	Bulgarian Personal Data Protection Act and Bulgarian Constitution There are also specific laws regulating video surveillance in specific contexts.	There are additional provisions to general GDPR rules setting out requirements with a view to clarifying the scope of the employee monitoring, obligations and methods of implementation.	Special rules with regard to data processing apply to employers that establish video surveillance monitoring systems in the workplace. There must be a legal ground for the use of such monitoring. Video surveillance is, however, mandatory in specific contexts (for example, banks and combustion plants). There is a general constitutional prohibition of email monitoring GPS tracking systems are accepted in specific cases and for legitimate purposes.
Croatia	Labour Act, Occupational Safety Act, National Implementation Act (implementing the GDPR) and sector-specific laws (for mandatory video surveillance)	There is an emphasis in the legislation on video and telephone surveillance. The involvement of the works council or trade union representative is mandatory when introducing new technology in the workplace or changes to modes of work. The consent of the works council or trade union representative is required if the monitoring is continuous. If it is not continuous, prior consultation is still required but a negative opinion is not binding.	It is not permitted to place monitoring devices in changing rooms, toilet facilities or other designated rest areas. Covert video and telephone surveillance is not permitted.
Cyprus	Law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data of 2018 (Law 125(I)/2018) The Commissioner for Personal Data Protection has issued guidelines on the use of video surveillance and biometric monitoring systems in the workplace.	Employee monitoring systems must be proportionate to the objective pursued. Electronic surveillance systems at the workplace can be installed for legitimate purposes only.	The use of biometrics for monitoring purposes is generally forbidden. Clocking systems using fingerprints or other biometric data are not allowed for the sole purpose of monitoring the presence or the working hours of employees. Covert surveillance is unlawful. Access to the content of personal emails and personal telephone calls of employees is prohibited.
Czechia	Civil Code (Act 89/2012), Labour Code (Act 262/2006 Coll.), Czech Data Protection Act (Act 101/2000 Coll.)	No special rules or limitations are stipulated in the Czech Data Protection Act in relation to consent granted by an employee to the employer. The act does not recognise a special category of employee personal data. The general consent rules apply to employee personal data. Employees must be duly informed about specific monitoring methods used by the employer.	Employee monitoring methods can be regarded as legal only in cases in which the employer has legitimate reasons for their implementation.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Denmark	Criminal Code, Personal Data Act, Television Monitoring Act (for video surveillance) and collective agreements	Monitoring of employees is permitted as long as it does not offend or harm employees or violate their human dignity and fundamental rights. Employees must be informed about monitoring and control measures before they are implemented in the workplace.	Data protection regulation and collective bargaining agreements outline restrictions on employee monitoring. Video monitoring is permitted to a certain extent, and it is generally considered to violate the conditions of reasonable and decent treatment of employees.
Estonia	Employment Contracts Act and Personal Data Protection Act	There are no detailed instructions with regard to an employer's monitoring rights, but guidelines have been issued by the Estonian data protection inspectorate. The Employment Contracts Act specifies quite generally that the employer is obliged to respect employees' privacy and verify the performance of their duties in a manner that does not violate employees' fundamental rights.	The use of surveillance equipment (for example, cameras) is permitted only for the purpose of protecting persons and property, but its use must be as minimal as possible and affect employees as little as possible.
Finland	Act on the Protection of Privacy in Working Life, Act on Cooperation within Undertakings, Act on Cooperation in Government Departments and Agencies, Act on Cooperation within Municipalities and Data Protection Act (*Tietosuojalaki* 1050:2018)	The employer is required by law to inform employees about the monitoring methods and agree on the monitoring rules in cooperation negotiations. Employers can process only personal data that are directly necessary for the employment relationship, thus limiting the scope of the monitoring activities, regardless of the extent of information given to employees.	Monitoring of employees' email correspondence is unlawful unless motivated on specific legal grounds. Strict conditions apply to the use of video surveillance. Its use is not permitted for the purpose of monitoring particular employees in the workplace. Monitoring by GPS tracking is allowed only during working hours. Cooperation negotiations are required for both CCTV monitoring and GPS tracking.
France	French Civil Code, Labour Code and French Data Protection Law	Strict compliance with the principles of transparency or loyalty, proportionality and relevance is required.	Specific requirements apply to the use of video surveillance, GPS tracking and biometric systems.
Germany	German Data Protection Act, Works Constitution Act and German Telemedia Act	There are strict boundaries to protect employees' privacy. The introduction and use of employee monitoring is subject to the approval of the works council.	Full monitoring of internet use and/or emails is allowed only in the case of a concrete suspicion of criminal activity or serious malpractice.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Greece	Law 4624/2019, Directive No. 115/2001 and Greek Constitution (Article 9a)	Greek jurisdiction does not differentiate between types of employee monitoring. Control and monitoring refer to the use of surveillance devices, in particular computers, surveillance circuits, sound recording, video recording and methods of monitoring employees' communications or movements to control them and/or their workplaces and work premises. Monitoring in the workplace is permitted under certain conditions.	Clarifications are given in guidelines issued by the Greek Data Protection Authority as detailed below. The monitoring of emails and internet use is permitted only in exceptional circumstances and when necessary to defend the legitimate interests of the employer. Video surveillance must not be used to monitor employees, unless justified by the nature of the professional activity. GPS tracking can be implemented for business optimisation and must not violate employees' privacy. The use of biometrics is permitted only to ensure workplace safety; there are no other instances in which biometrics can be used.
Hungary	Hungarian Labour Code and Hungarian GDPR Implementation Act	The legal basis for monitoring employees is, in most cases, when the employer has a legitimate interest. The employer must conduct a balancing test, weighing its legitimate interests against employees' rights and freedoms.	Covert monitoring is illegal, the use of CCTV must be justified, the monitoring of internet usage and emails is subject to restrictions, biometric entry systems are permitted only in exceptional cases and GPS tracking is not permitted to determine the whereabouts of employees outside their working hours.
Ireland	Data Protection Act 2018	Any employee monitoring must be proportionate and necessary to safeguard the employer's legitimate interest but without prejudice to the rights and freedoms of the employee.	
Italy	Workers' Statute (Article 4 of Italian law 300/1970) amended by labour reform in 2015 (Article 23 of legislative decree 151 of 14 September 2015) and Privacy Code (legislative decree 196/2003) amended by legislative decree 101/2018	Remote control devices can be used only for legitimate purposes and specific reasons, such as organisational and production needs, work safety and the protection of the enterprise's assets. Their use must be covered by specific collective agreements or administrative authorisation and they must conform to data protection legislation.	Direct monitoring of work activities carried out remotely by means of installed devices is prohibited without exception. Case law and administrative practice have introduced specific limits depending on the form of monitoring.
Latvia	Personal Data Processing Law, adopted on 21 June 2018	The principles of legitimacy and proportionality between workers' rights and the employer's interests apply. Employees' right to privacy needs to be taken into account when installing video surveillance and other forms of monitoring.	Video monitoring and audio recording should be explicitly motivated. Video surveillance systems can be used for monitoring workers' performance only in very specific cases.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Lithuania	Article 27 of Labour Code No. XII-2603 regulating the protection of employees' right to a private life and of personal data, and law XIII-1426 amending law I-1374 on the legal protection of personal data	In principle, employers have the right to use control measures to monitor employee performance at the workplace, but only if this right is clearly established and justified in the internal regulations of the company. The employer must inform employees about the internal regulations on employee monitoring (against signature or by any other means of proof).	
Luxembourg	Labour Code (Article L 261-1) and law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general rules on data protection	There is no legal definition of surveillance. Employers can undertake surveillance for any purpose, provided that they comply with a number of conditions set by the law. The employer must provide prior information to the employees concerned and their representatives. The employees have the right to appeal to the National Commission for Data Protection if the conformity and legitimacy of the processing is in doubt.	
Malta	Data Protection Act of the Laws of Malta (Cap 440) and its subsidiary legislation, and guidelines issued by the Office of the Information and Data Protection Commissioner	There is no specific regulation on employee monitoring and surveillance in the workplace. The data protection rules and principles set out in existing legislation apply. Monitoring is therefore permitted provided that it is adequate, relevant and not excessive and that it is implemented in the least intrusive way possible. Adverse consequences of monitoring must be justified by its benefit to the employer and/or to others. Although express consent for monitoring is not usually required, the employer should inform the employees about the following: (1) that monitoring is being carried out, (2) the purposes of such monitoring and how their personal data may be used, (3) who will be provided with the personal data (4) if certain behaviour by the employee may result in disciplinary action.	It is advised that, before implementing biometric systems, a privacy impact assessment should be carried out to ensure that the use of biometrics is necessary.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Netherlands	General Data Protection Regulation	There is no set definition of employee monitoring and/or surveillance. The employee's consent is not considered a valid ground for processing personal data. Employee monitoring is not prohibited, but employers must take into account the privacy of employees. Employee monitoring is permitted if it meets the conditions of the GDPR. These conditions concern the legitimate interest of the employer outweighing employees' privacy, the proven necessity of the monitoring, prior consent of the employees and permission of the works council.	Covert surveillance of employees is permissible only under certain conditions. Video monitoring and surveillance (including use of facial recognition technologies) to establish patterns of behaviour are generally not permitted GPS tracking is permitted only to ensure employees' safety, prevent theft or in the case of a suspicion of criminal activity.
Poland	Labour and Civil Codes, and Act on the Protection of Personal Data	Monitoring refers to the workplace only (not monitoring of employees). The provisions in the Labour Code explicitly relate to video monitoring and monitoring of emails but are also applicable to 'other forms of monitoring'. Employers must define the scope, method and purpose of the monitoring in collective agreements or internal regulations.	Monitoring of emails cannot infringe correspondence secrecy and other personal rights of employees. Monitoring of private emails is prohibited. Video monitoring is permitted in specific circumstances and when it is justified.
Portugal	Labour Code (law 7/2009 of 12 February) and Portuguese Data Protection Act (law 58/2019 of 8 August)	The general principle that employees have a right to privacy applies. Remote surveillance systems may be used only for the purpose of protecting workers, clients and properties and not for controlling the professional performance of workers. The employer is obliged to notify employees on the terms and restrictions of use of company equipment and data processing.	Monitoring of employees' activity through the use of email, internet and/or biometric devices is not permitted. The employer is prohibited from using the consent of their employees to process personal data when such processing results in a legal or economic advantage for them.
Romania	Labour Code (law 53/2003), law 190/2018 on measures to implement Regulation (EU) 2016/679, and Decision 99/2018 of the National Supervisory Authority for the Processing of Personal Data	Law 190/2018 stipulates that employee monitoring is permitted if a set of cumulative conditions is fulfilled. These conditions comprise (1) the legitimate interests pursued by the employer, which must be fully justified and prevail over the interests or rights and freedoms of the employees, (2) the preliminary information given to the employees, (3) the consultation of the trade union or of the representatives of the employees before introducing the monitoring systems, (4) the exhaustion of other, less intrusive, forms and modalities of monitoring means and (5) the period of storage, which must be proportional to the purpose of processing, but not more than 30 days.	According to the laws currently in force, the employer has no right to supervise its employees in the workplace. However, if the activity is carried out in open spaces, where dozens of employees work, in industrial halls or in supermarkets, the employer may set up surveillance cameras, for security reasons. However, these must be in sight, and employees must know about their existence.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Slovakia	Labour Code (Act 311/2011 Coll.), Act on Personal Data Protection (Act 18/2018 Coll.) and amendments to certain acts	If an employer implements a monitoring mechanism, the employer must consult with the employees' representatives on the extent of control, method of implementation and duration. If there are no employee representatives at the employer, the employer proceeds autonomously in accordance with the rules of law.	An employer must not, except for specific reasons relating to the specific character of the employer's activities, intrude upon the privacy of an employee in the workplace by monitoring them, keeping records of telephone calls and checking email correspondence without giving advance notice.
Slovenia	Employment Relationships Act, Personal Data Protection Act, Information Commissioner Act and Electronic Communications Act	The employer must protect and respect employees' privacy. Employee monitoring is permitted, but the employer must inform employees in advance and in writing about the exercise and methods of supervision. Employees' consent is required unless the monitoring can be justified on objective grounds.	Video surveillance of 'working spaces' is permitted only in exceptional cases and for a legitimate aim, for example, safeguarding people or property, protecting an employer's business secrets or when this cannot be achieved by other means. Recording and listening to telephone conversations are not explicitly regulated, but generally are not permitted. The employer is allowed to process only personal data that is directly necessary for managing the employee's employment relationship.
Spain	Spanish Digital Rights Act (Organic Law 3/2018 on the protection of personal data and guaranteeing digital rights)	A new concept of 'digital rights' has been introduced in Spanish jurisprudence.	
Sweden	Camera Surveillance Act, Employment (Co-Determination in the Workplace) Act (1976:580) and Data Protection Act (2018:218)	There is no specific regulation on employee monitoring and surveillance at the workplace.	The surveillance of employees with the help of CCTV is allowed only when there are compelling reasons for this (for example, reasons to suspect that employees are committing crimes). An employer who wants to set up a camera surveillance system at a workplace is obliged to negotiate with employee representatives. This is regulated in sections 11–14 of the Employment Act.

Country	Relevant legal documents	Country specificities	Restrictions on the use of employee monitoring
Norway	Working Environment Act relating to working environment, working hours, employment protection (chapter 9) and Personal Data Act (national implementation of the GDPR) There is a 'basic agreement' between the social partners the Norwegian Confederation of Trade Unions (LO) and the Confederation of Norwegian Enterprise (NHO), including supplementary agreements on control measures in enterprises	Although workplace monitoring is regulated in the Working Environment Act, the term itself is not legally defined. Legislative sources, including draft resolutions presented to the parliament, nonetheless mention specific technologies, including timesheets, access control, performance monitoring, quality control, drug testing, medical tests, checks of bags or lockers, camera surveillance, electronic sensors and monitoring of emails.	Employee monitoring is restricted by employees' right to privacy. The employer must demonstrate a legitimate and continuing need, and the measure must be proportional. Employees must be informed and the measure must be discussed with shop stewards.
UK	Human Rights Act 1998, Data Protection Act 1998, Employment Practices Data Protection Code, Regulation of Investigatory Powers Act 2000 and Telecommunications Regulations 2000	As most forms of employee monitoring involve the processing of personal data, such monitoring activities must comply with data protection principles and rules.	According to the Employment Practices Data Protection Code, covert surveillance is in principle prohibited and allowed only in the case of a concrete suspicion of criminal activity or serious malpractice.

Source: *Network of Eurofound Correspondents*

Role of collective bargaining

Employee monitoring and the processing of data resulting from this monitoring are regulated in legislation and, in a number of countries, also through collective agreements. There are several instances of collective agreements at national intersectoral level. A case in point is Belgium, which has longstanding national collective bargaining agreements regulating specific forms of monitoring, for example video surveillance (collective agreement No. 68 of 16 June 1998) and the electronic monitoring of internet and emails (collective agreement No. 81 of 26 April 2002). Addressing more general monitoring issues, in Norway, the central 'basic agreement' between the LO and the NHO contains a supplementary agreement (LO and NHO, 2019) on monitoring activity in enterprises. Among other things, this stipulates that the design, implementation and evaluation of control measures must be subject to social dialogue with employee representatives.

In some Member States – such as Austria, Croatia, Denmark, France, Germany, the Netherlands and Sweden – and in Norway, bargaining or consultation surrounding employee monitoring is promoted by legislation, giving works councils or other employee representatives powers in this area. In Austria, only monitoring measures that do not affect workers' human dignity (for example, recording working time) can be implemented unilaterally by employers. All other monitoring measures having an impact on human dignity are subject to co-determination via the works council or an individual agreement with the employees in the absence of a works council. In Croatia, the Labour Act has provisions that apply to employee monitoring; it stipulates that the involvement of the works council (or a trade union representative in the absence of a works council) is mandatory when implementing measures related to health and safety at work, introducing a new technology in the workplace or implementing changes to the organisation and/or mode of work. Similar to the situation in Austria, in Germany the works council has a co-determination right on monitoring by means of techniques such as CCTV and GPS tracking. The works council's prior consent is also required in the Netherlands if the employer intends to adopt, amend or withdraw policies concerning, among other things, data privacy and employee monitoring. Specific forms of monitoring such as video surveillance and GPS tracking are addressed in Finland in the cooperation procedure and are subject to cooperation negotiations (Ministry of Economic Affairs and Employment in Finland, undated). In France, the employer is obliged by law to consult the works council over any introduction of new technology within the company if this might affect employees' working and employment conditions. The employer must also inform the Social and Economic Committee (CSE)[4] about new techniques and automated systems for enabling the monitoring of employees' activities prior to their introduction and implementation in the workplace. In Sweden, according to the Employment (Co-Determination in the Workplace) Act, employers are required to negotiate with trade unions regarding any significant changes in their activities, including the introduction of digital surveillance in the workplace. In Romania, information and consultation

4 Following a reform of the French Labour Code (2017), the works council (CE) was replaced by the CSE.

with the relevant trade unions or other employee representatives is one of the cumulative conditions to be fulfilled by the employer before introducing employee monitoring in the workplace.

Recent changes to legislation

In a number of countries, legislation related to employee monitoring has undergone some changes in recent years. In Italy, the amended provisions in the Workers' Statute stipulate that the use of remote control devices must be covered by specific collective agreements or administrative authorisation and must conform with data protection legislation.[5] By law, remote control devices can be used only for legitimate purposes and for specific reasons – such as organisational and production needs, for work safety and for the protection of the enterprise's assets – and by no means can they be used as a tool for the surveillance of individual workers.

In other EU Member States (Bulgaria and Estonia, for example), relevant legislation on employee monitoring is more permissive, albeit special rules apply to more intrusive forms of monitoring, such as video surveillance and GPS tracking. It is, however, generally accepted in Bulgaria that the employer has the right to install surveillance and control systems (including GPS tracking) if this is justified by the nature of the activity performed or for security reasons. In Czechia, at corporate level, especially in large companies, the usage of electronic surveillance equipment is usually governed by means of internal company regulations.

In Poland, following the implementation of the GDPR, specific provisions were introduced in the Labour Code regarding monitoring in the workplace and regulating specific forms of monitoring.[6] The existing provisions explicitly relate to video monitoring and monitoring of email correspondence, but also apply to 'other forms of monitoring' (not specified in the legislation). As regards video surveillance, the Polish Labour Code stipulates that the employer is obliged to inform employees about this form of monitoring no later than two weeks before its implementation. In this regard, the Polish Ministry of Family, Labour and Social Policy released a statement in 2018 stating that video surveillance can be introduced by a unilateral decision of the employer in situations where negotiations with establishment-level trade unions have been inconclusive over a 30-day period.

In Romania, the implementation of the new GDPR in national legislation (law 190/2018) has resulted in more stringent provisions on employee monitoring, especially video surveillance. It is estimated that before the entry into force of these normative acts, about 47% of employees in Romania were monitored (Evz.ro, 2008). In addition, in Slovakia, relevant legislation on employee monitoring has been reinforced by the adoption of the new Act on Personal Data Protection and following the amendment of the Labour Code. According to the new legislation, employers can resort to employee monitoring only if there is a compelling reason for doing so. By law, the employer must consult with employee representatives (trade unions or the works council) on the use of employee monitoring systems, but their consent is not mandatory.

As regards Hungary, the most significant change following the implementation of the GDPR was the explicit prohibition of the use of company-owned ICT devices by employees for private purposes. Before the implementation of the GDPR, employees could use laptops, mobile telephones and other work devices for personal purposes, unless private use was explicitly prohibited by the employer. This has now changed and, by default, employees can no longer use ICT tools and devices for private purposes, unless otherwise specified in specific agreements with the employer.

In other EU Member States, such as Luxembourg, recent changes to national legislation surrounding employee monitoring and surveillance have made such practices less restrictive. Following the implementation of the GDPR, the notion of surveillance has been omitted from the new provisions in the Labour Code (repealing the law of 2 August 2002) and greater flexibility is now given to employers with regard to employee surveillance (provided that a number of conditions are fulfilled).[7] The omission of the definition of surveillance in the Labour Code was contested by the Chamber of Employees of Luxembourg (CSL) during the parliamentary work and criticised for creating legal uncertainty.

Recommendations and guidelines

National data protection authorities in EU Member States play an important role in clarifying the relevant legislation and have issued opinions, guidelines and good practices on employee monitoring in general, as well as on specific forms of monitoring in the workplace.

In France, the national Data Protection Authority (CNIL) has published several recommendations and opinions that apply specifically to the employment context and provides guidance in respect to various forms of monitoring. These include video surveillance, recording of and listening to telephone conversations, access control to the work premises and monitoring of working hours, GPS tracking, the use of ICT tools for the recruitment and management of staff, and monitoring of employees' computers.

In consideration of the intrusive nature of video surveillance, guidelines are often issued to provide clarifications on the lawful conditions of this form of monitoring. For example, in Hungary, national legislation

5 Amended by the labour reform (the so-called Jobs Act) in 2015 (Article 23 of legislative decree 151 of 14 September 2015). Before the Jobs Act, the provisions were more restrictive, and remote monitoring and surveillance were explicitly forbidden. The changes to the legislation were intended to take into consideration technological and organisational changes; however, the regulatory framework remains strict, as it prohibits existing technologies from being used as tools for the surveillance of individual workers.

6 In the Polish Labour Code, monitoring refers to the workplace and there is no specific mention of 'employee monitoring'.

7 The definition of surveillance in the repealed provision of the Labour Code was the following: 'any activity which, by means of technical instruments, consists in the non-occasional observation, collection or recording of personal data of one or more persons relating to behaviours, movements, communications or the use of electronic and computerized devices' (Article 2(q) of the law of 2 August 2002).

leaves the specifics of video surveillance open to interpretation; therefore, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) has set out specific requirements for and restrictions to its use.

In Cyprus, the guidelines issued by the Commissioner for Personal Data Protection specifically address the use of biometric systems for employee monitoring purposes, which is not addressed in legislation. As regards employee monitoring in general, the common practice in Cyprus is for social partners to solve their differences through collective bargaining and, when this is not possible, the trade unions or individual employees raise a complaint with the Commissioner. Recent complaints and enquiries in relation to the use of software for monitoring employees' computer activities have prompted the Commissioner to publish guidelines in this regard. These guidelines state that the employer can monitor some computer activities under specific circumstances and in compliance with specific regulations, but the monitoring of all computer activities or private email correspondence is not permitted.

In Greece, as the jurisprudence does not differentiate between different forms of monitoring, the Hellenic Data Protection Authority (HDPA) has issued several guidelines to clarify the conditions under which the employer can resort to specific forms of monitoring in the workplace. These include the monitoring of employees' emails and internet use, video surveillance, GPS tracking and biometric methods.

In the absence of specific legislation regulating different forms of monitoring, the Maltese Office of the Information and Data Protection Commissioner (IDPC) has also published guidelines to instruct employers on the permissible methods of monitoring and surveillance. Similarly, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, AP) provides guidelines with regard to various types of monitoring practices and makes a distinction between surveillance (*toezicht*) and monitoring (*controle*), linking both explicitly to the privacy of employees.

The Norwegian Data Protection Authority has produced several statements on workplace monitoring and surveillance and raised concerns about the erosion of trust in working life resulting from employee monitoring. The authority notes that the legislation concerning workers' right to privacy and their right to be informed about what data are gathered about them is often not adhered to by employers, although current legislation is largely sufficient. The director of the Norwegian Data Protection Authority has argued that the problem often lies with the attitudes and limited knowledge of many employers (Thon, 2015). According to a recent survey conducted in Norway among 140 employers, a significant proportion of them do not fully comply with regulations concerning workplace monitoring – 36% report not having guidelines in place on the use of monitoring and surveillance (Deloitte, 2019). Nearly 6 out of 10 of the employers surveyed reported that monitoring in the company had not been discussed with the employees.

National legislation in the UK is supported by the Employment Practices Code, published by the Information Commissioner (the national data protection authority), which deals specifically with workplace monitoring. While the code is not legally binding, it may be relied upon in any proceedings where there is an alleged breach of the UK Data Protection Act. The Employment Practices Code emphasises that employees must be informed about the monitoring carried out in the workplace and this must be proportionate and take into account employees' privacy. Whether monitoring is deemed reasonable and proportionate or not will depend on such issues as the purpose of the monitoring, the probable adverse effect of the monitoring, if there are any alternatives that will achieve the same objectives and whether or not, on balance, the monitoring is justified. The Employment Practices Code also identifies problems with the notion of consent in the employment relationship.

Regulatory compliance

With the new GDPR, data protection legislation has become a substantial element in the regulation of employee monitoring and surveillance in EU Member States. Regulatory compliance is monitored and guaranteed by independent public supervisory authorities. Such authorities also deal with complaints in relation to potential breaches of data protection rules, carry out inspections and impose administrative sanctions where necessary.

According to the 2018 annual report of CNIL, 17% of complaints received in 2018 in France concerned employment issues. Technological surveillance (including video surveillance, geolocation and cybersurveillance[8]) is a concern among employees in both the private and the public sectors. The number of complaints led CNIL to write to the Minister of Labour in December 2018, warning against the risks involved in the remote surveillance of employees. Such practices can lead to placing people under permanent surveillance and can potentially be used as a form of psychological harassment (CNIL, 2018).

The implementation of the GDPR in national legislation has, in some cases, brought some changes to the role of these public bodies. In France, before the entry into force of the GDPR, CNIL issued an authorisation to employers for the processing of personal data in the context of employee monitoring activities. The control of personal data processing is now done *a posteriori*.

Similarly, in Luxembourg, the National Data Protection Commission (CNPD) no longer issues prior authorisations to employers who intend to carry out employee monitoring. This was previously required by law and served as a form of 'compliance in principle' or upstream control. The abolition of the prior authorisation requirement is nonetheless offset in the amended

8 According to the definition given by CNIL, cybersurveillance involves a device set up by an employer to control the use of information and communication technologies by employees.

legislation by the obligation on employers to document the compliance of their processing with the law in the event of a review or inspection. The CNPD continues to monitor compliance and issues administrative penalties and fines in the case of infringements.

In Czechia, it is the role of the State Labour Inspection Office to ensure compliance with provisions that, among other things, regulate employee monitoring. An amendment to Act 251/2005 Coll. on labour inspection, which came into force on 29 July 2017, allows labour inspectorates to sanction employers for undue interference with the privacy of employees.

With specific regard to remote working, which many employers have authorised during the COVID-19 pandemic to keep businesses going, the president of the Italian Data Protection Authority (GPDP) has underlined, in a hearing to the national parliament, the risks arising from remote working and the monitoring and surveillance possibilities that this entails:

> *The intensive use of new technologies to perform work cannot … represent an opportunity for the systematic and ubiquitous monitoring of the worker, but must take place in full compliance with the guarantees enshrined in the Statute protecting self-determination, which requires above all the provision to workers of adequate training and information about the treatment of their data.*
>
> (GPDP, 2020)

Since the implementation of systematic and pervasive monitoring of workers' tasks cannot be considered necessary to perform the work, the president of the GPDP is of the view that it would be illicit to install such a system on work devices. Moreover, the right to disconnect must be guaranteed – for example, by introducing stricter rules.

In compliance with Article 35(4) of the GDPR regulation, the data protection authorities of many EU Member States have already published lists of 'high risk' data processing activities requiring a data protection impact assessment and relating to employee monitoring. The Romanian National Supervisory Authority for Personal Data Processing is one of the national authorities to have issued such a list. This list indicates data processing activities for which an impact assessment is mandatory (Decision No. 174 of 18 October 2018), including large-scale data processing using new technologies, with a specific reference to data generated by sensor devices, for example, IoT devices. An impact analysis is required for employers who systematically monitor the activities of their employees – for example, on the internet and at workstations – by means of workplace surveillance through CCTV systems or the tracking of business vehicles or devices used by employees who work outside the office. The data protection impact assessment is carried out by the National Supervisory Authority for Personal Data Processing. In addition, the Irish Data Protection Commission published, in 2018, a list of circumstances in which a data protection impact assessment is required. The use of new or novel technologies is explicitly listed among the factors indicative of high-risk data processing.

Decisions issued by national data protection authorities

National data protection authorities can also issue decisions and fines in cases of employee monitoring. For example, the Norwegian Data Protection Authority (Datatilsynet) issued a €10,000 fine in 2013 to a company checking timesheets against GPS data. In 2018, another case that received media attention concerned the use of remote transaction monitoring, including screen capture and audio recording of 400 customer service employees at the telecommunications company Telenor, which the local social partners were in disagreement over. The Norwegian Data Protection Authority assessed the case and deemed the practice illegal, prompting Telenor to discontinue the monitoring with immediate effect (Datatilsynet, 2019).

A number of cases brought to the attention of the GPDP in Italy concern the use of different digital devices, including wearables, which allow the geolocalisation of workers, directly or indirectly through the combination of data on shifts with data collected through digital devices. According to the Italian Data Protection Authority, such systems must not be used for the constant monitoring of workers. Workers must also be informed and made aware of the presence and activation of such monitoring systems and must be informed about the nature of the data collected and their use.

In Greece, a case that made the news in 2019 concerned the accounting firm Pricewaterhouse Coopers (PwC), which was found by the Hellenic Data Protection Authority (HDPA) to contravene the GDPR in relation to the processing of its employees' personal data. The HDPA imposed a fine on PwC of €150,000. Before the GDPR came into force, PwC requested its employees to sign a document consenting to the processing of their personal data for a variety of purposes, including for monitoring purposes. According to the current GDPR rules, employee consent is not an appropriate legal basis and PwC should have refrained from processing its employees' personal data once the GDPR came into effect.

In the Netherlands, the AP has also issued a number of decisions and judgments in relation to infringements of privacy rights and data protection rules resulting from employee monitoring. For instance, the AP ruled as unlawful the use of secret camera surveillance used by the consumer electronic retailer Media Markt Netherlands for reviewing the performance of individual employees (AP, 2013), although the stated goal of the monitoring activity was the protection of company assets and ensuring employees' safety. The AP took a similar stance in the case of the transport and logistics company De Rooy Transport, which used event data and video recording of drivers, ostensibly to improve road safety. In this case, the AP also deemed that the use of this monitoring system was unlawful and ordered the company to discontinue it, asserting that the drivers' right to privacy had priority over the road safety arguments (AP, 2015).

Court rulings

Key judgments of the European Court of Human Rights

Standards in relation to the protection of privacy, including in the context of the employment relationship, have been established by international human rights protection bodies, most notably the European Court of Human Rights (ECtHR). The often-cited case of *Bărbulescu* v *Romania* has important implications for the jurisprudence on employee monitoring and surveillance. The case concerned the dismissal of an employee for using a work email account for personal purposes during working hours, in violation of internal company regulations (ECtHR, 2017). The judgment issued in 2016 by the ECtHR reversed the previous judgments and ruled against the dismissal, as the dismissal was deemed to be in breach of the right to a private life and private correspondence set out in Article 8 of the European Convention on Human Rights.[9] Article 8 is generally used across national jurisdictions to protect employees' privacy in the employment context. The ECtHR judgment in relation to *Bărbulescu* v *Romania* sparked numerous reactions in the media but was generally welcomed for establishing a level of protection for employees and for setting boundaries in the context of the digitalisation of work, as this digitalisation is generally leading to an increasing blurring of boundaries between work and family life.

Until the decision in *Bărbulescu* v *Romania*, one of the most prominent cases concerning employee monitoring was *Copland* v *the United Kingdom* (ECtHR, 2007). In this case, Copland's telephone calls, email correspondence and internet use were monitored by her employer under the suspicion that she had been using the employer's facilities for personal purposes. Similarly to the *Bărbulescu* v *Romania* case, on this occasion, the ECtHR found that the employer had violated the employee's right to a private life and private correspondence under Article 8 of the European Convention on Human Rights. These ECtHR judgments show that the protection granted by Article 8 extends to the workplace and that the employee should receive proper and prior information on the scope and nature of surveillance. At the same time, the employer should justify the measures implemented and minimise surveillance where possible, for example, by using the least intrusive methods. An important aspect in this regard is the balance between the employer's legitimate interest and the privacy rights of employees. This applies to all forms of monitoring and surveillance, not just monitoring of personal communication in the workplace.

Another recent case brought to the ECtHR was the *Antovic and Mirkovic* v *Montenegro* case, which involved two professors teaching at the University of Montenegro where video surveillance systems were installed in the teaching auditoriums (ECtHR, 2018). The ECtHR confirmed that the video surveillance constituted interference with their privacy rights under Article 8 of the European Convention on Human Rights.

With regard to video surveillance, another recent ECtHR court ruling concerns the *López Ribalda and Others* v *Spain* (ECtHR, 2019) case, which established that covert video surveillance of employees can be justified when there is a reasonable suspicion of serious misconduct. In this case, supermarket employees were suspected of theft, and evidence from hidden cameras confirmed the suspicion, resulting in the dismissal of the employees on disciplinary grounds. The ECtHR found no violation of Article 8. Covert surveillance is, however, not allowed for minor suspicion of wrongdoing committed by employees.

Judgments of national courts

National courts have, on several occasions, ruled in favour of employees who have been the subject of unjustified monitoring, tracking and surveillance. The case law in EU Member States shows that it is not enough for an employer to provide evidence collected through employee monitoring to prove that an employee is to blame, such as in the non-performance of certain functions. For instance, according to a ruling issued by the Vilnius Regional Court in 2012, the dismissal of an employee for using Skype during working hours for private conversations and using the internet for non-business purposes was unlawful. The court supported the employee's argument that the employer could not base the lawfulness and validity of the imposed penalty on Skype extracts and data retrieved from the employee's work computer and held that such data were obtained in violation of the employee's legitimate expectation of and right to privacy.

A similar judgment was reached by the German Federal Labour Court in 2017, which revoked an employee's termination owing to the excessive private use of a work computer, which was monitored via keylogger software. The employee admitted having used the computer for private purposes mostly during break times, but she was nevertheless terminated without notice. The judge declared the employee's termination invalid because the use of the keylogger software was deemed to be excessive and disproportionate in the absence of previous suspicion of a crime.

In Austria, the Supreme Court assesses monitoring measures primarily for their impact on human dignity. In a court case in 2013, a service technician of a heating technology company removed an electronic tachograph that the employer had installed in the company vehicle without the employee's consent. Following this, the employer dismissed him, upon which the employee went before the court. The Vienna Higher Regional Court ruled in favour of the employee, judging the dismissal to be unjustified. The court deemed that the device could have been used to determine the exact position of the employee, which represented a permanent performance check and thus encroached upon the personal freedom of the employee and had an impact on human dignity.

9 Article 8 states that 'everyone has the right to the protection of personal data concerning him or her' and provides that interference with this right is allowed only in accordance with the law and when it is necessary in a democratic society to pursue a legitimate aim.

There are situations in which intrusive monitoring is justified and legitimate. A case on which the Irish Workplace Relations Commissioner was consulted in 2018 involved an employer who had installed a camera on the truck of a driver working for him. The video recorded only the fuel usage and showed the driver had been siphoning fuel for private use and, as a result, he was dismissed. The Commissioner ruled that the dismissal in this case was lawful, stating that covert surveillance – as in this case – may be justified when there is a concrete suspicion of fraud or serious breach of duty.

With technological advances, there are new and more intrusive ways to monitor workers. There are, for example, increasing concerns surrounding the use of digital wristbands and GPS tracking devices, which allow workers to be located in real time and notifications to be sent when a task is accomplished. There have already been some court judgments in this regard. For example, the Spanish National Court has sided with the riders of fast food chain Telepizza, who contested the use of a geolocation application on their own smartphones. The measure was deemed unlawful for violating the privacy of employees and not respecting the right to information and consultation of union representatives. The judgment also annulled the clauses introduced in employees' new contracts that had been stipulated in February 2019 on the use of GPS tracking.

Positions and views of the social partners

At European level, the ETUC has voiced concerns about the risks arising from the use of new technologies for employee monitoring and surveillance, especially as regards their implications for workers' fundamental rights. In its resolution on digitalisation, the ETUC called for an EU directive on privacy at work, based on respect for human dignity, privacy and the protection of personal data (ETUC, 2016). Other international and European trade union federations – for example, UNI Europa ICTS (the information, communications, technology and service section of the European trade union federation for service workers) and the Trade Union Advisory Committee to the OECD – have also made demands to be involved in negotiations related to the introduction of state-of-the-art technologies in the workplace, including AI (ETUI, 2020).

The global union federation for skills and services, UNI Global Union, has raised concerns in particular around the increasing use of algorithmic management tools, which, among other things, create new forms of surveillance in the workplace (UNI Global Union, 2020). Such tools cover a range of technologies and applications, from software that tracks employees' working time to machine learning and AI-enabled applications that assign work tasks, predict employees' behaviour and guide day-to-day decision-making in the workplace. As part of its campaign for a more ethical implementation of these tools, UNI Global Union has released an algorithm management guide, advocating for greater employee involvement in the way algorithmic management is implemented and calling for unions to negotiate with employers and create 'algorithmic use agreements', which take into account issues around transparency, accountability, proportionality, fairness and access to data.

From an employer perspective, BusinessEurope has welcomed the adoption of the GDPR, but also noted that the 'application of all legal data processing possibilities should be permitted instead of forcing one method' and urged the Commission to understand 'the impact of the GDPR in relation to its ambitions to boost European excellence in artificial intelligence' (BusinessEurope, 2020b). The other major EU-level employers' organisation, the Association of Crafts and SMEs in Europe (SMEUnited, formerly UEAPME), has raised concerns in relation to requirements arising from the implementation of the GDPR that are considered burdensome and that lead to high costs for small and medium-sized enterprises (SMEs; SMEUnited, 2019).

The European social partners have found some common ground in the wider debate on digitalisation with the adoption of the autonomous framework agreement on digitalisation in June 2020 (ETUC et al, 2020). Among the many implications of digitalisation for work, the document recognises that the use of digital technologies and AI surveillance systems poses new risks, potentially compromising human dignity and contributing to a deterioration of working conditions. The agreement also recalls Article 88 of the GDPR and the possibilities to establish more specific rules in collective agreements on the protection of the rights and freedoms in relation to the processing of personal data in the context of the employment relationship. The adoption of the agreement marks the beginning of the five-stage implementation process; it is an important milestone, as it sets the tone for negotiations at national level and proposes concrete measures – to be adapted to local needs – to address the many impacts of digitalisation in the workplace.

At national level, trade unions in some countries have been particularly vocal about issues arising from the use of new technologies for employee monitoring, condemning intrusive practices. For instance, French trade unions have released statements on the risks associated with digital employee monitoring. With regard to pilot testing of facial recognition technology initiated in 2019 in two high schools in Nice and Marseille, the French General Confederation of Labour (Confédération Générale du Travail, CGT) made the following plea:

> *For artificial intelligence and the use of big data in the service of humanity and social progress and not as the armed arm of an authoritarian capitalism against which the CGT calls and will continue to call for determined and systematic resistance.*
>
> (CGT, 2019)

In France, trade unions have also been very active in negotiating for workers' rights in the context of the increasing digitalisation of work. An outcome of such pressure is the law introduced in 2016 giving employees the right to disconnect outside working hours (Eurofound, 2020c).

In the UK, the Trades Union Congress (TUC) has taken a firm stance on employee monitoring, stating that, while some degree of monitoring is a normal part of working life, there are legal limits on intrusive monitoring and surveillance. The TUC argues that, in recent years, cheap monitoring technology has made it easier for employers to collect information about their staff. In its policy recommendations, the TUC calls for trade unions to have a legal right to be consulted on and to agree in advance to the use of electronic monitoring and surveillance at work (TUC, 2018). The TUC also demands an update to the Employment Practices Code to take account of new technologies and to make it legally binding for employers. Both the TUC and the Confederation of British Industry (CBI) have expressed concerns about the prospect of British companies implanting staff with microchips to ensure security. A spokesperson for the CBI commented, 'While technology is changing the way we work, this makes for distinctly uncomfortable reading. Firms should be concentrating on rather more immediate priorities and focusing on engaging their employees' (The Guardian, 2018a).

The policy debate on employee monitoring in Spain mainly revolves around data protection issues. The Spanish General Union of Workers (UGT) has published some guidelines for collective bargaining in relation to data protection and guaranteeing so-called 'digital rights' (UGT, 2019a). According to the UGT, it is necessary to strengthen the role of collective agreements with a view to protecting workers' rights in relation to the use of data. In 2018, UGT Catalunya produced a detailed analysis on the relationship between new technologies and workers' privacy rights, reiterating that the use of technological devices by the employer for monitoring purposes must be agreed with workers and adapted via collective bargaining (Ezquerra, 2018). The UGT has also expressed more general concerns in relation to the implications of the use of new technologies for working conditions and particularly workers' health and safety (UGT, 2019b). These concerns are also reflected in the Spanish Strategy for Health and Safety at Work 2015–2020 which refers to the risks arising from new digital technologies, noting that ICT-based work practices (including teleworking) give rise to the use of worker surveillance programs (INSHT, 2015).

The topic of employee monitoring and surveillance has generated a controversial debate in Germany: on one side are those advocating for technological advances for business benefits and on the other side are those criticising employee surveillance for violating privacy and data protection rights. With regard to recent changes to the regulatory framework surrounding employee monitoring, trade unions have expressed some dissatisfaction with the existing provisions for creating legal uncertainties. The German United Services Trade Union (ver.di) has called for a clearer set of rules on workplace monitoring and surveillance, while the Confederation of German Trade Unions considers that the provisions on video surveillance continue to be inadequate in spite of the recent revision of the Data Protection Act.

In Croatia, the trade union for the printing and publishing industry has also warned against the use of surveillance equipment at the workplace, which is becoming a bigger source of concern, especially in relation to the greater capabilities for the collection, storage and processing of digital data (Croatian Graphical Union, undated). For example, data obtained from video surveillance can be linked to other employee data collected via other forms of monitoring, creating a very powerful integrated system of information available to the employer at any moment. According to the trade union, video surveillance systems used for remote employee monitoring should not be permitted.

In Luxembourg, the more general debate around the implications of digitalisation also touches on the issue of monitoring in the workplace. The government established, in 2018, a dedicated ministry on digitalisation, led by Prime Minister Xavier Bettel and Minister Delegate to Digitalisation Marc Hansen. The social partners are said to be in talks with the government, and the Luxembourg Confederation of Christian Trade Unions has expressed concerns about the consequences of technological advances, including their impact on employee monitoring.

Employee monitoring is debated in Norway every so often. In 2018, the Norwegian government announced the intention to create a new privacy commission and to initiate a public hearing to determine its mandate. The public hearing produced a variety of statements from relevant actors, with trade unions expressing most concern about employee monitoring and surveillance. The Norwegian Confederation of Trade Unions (LO), the Federation of Norwegian Professional Associations (Akademikerne) and the Norwegian Confederation of Unions for Professionals all released statements stressing the importance of privacy in working life and called for this to be specifically included in the mandate of the commission (Regjeringen, 2018). The Federation of Norwegian Professional Associations argued that new technologies are increasing monitoring and surveillance capabilities, which is challenging privacy and trust at the workplace. The LO stated that it had observed a worrying increase in the monitoring and surveillance of workers and that it was concerned with how privacy regulations are being implemented and the lack of oversight. The LO's 2017 action programme also underlined that monitoring and surveillance at work threatens privacy, creates stress and lowers the influence of employees, and called for strengthening laws and collective agreements in this field. In a similar vein, the Norwegian Confederation of Unions for Professionals stressed the need for the protection of workers' privacy, arguing for the creation of a permanent legislative council to assess the need for safety measures in relation to digitalisation.

In many other countries – especially in eastern EU Member States – the topic of employee monitoring is not high on the policy agenda of the social partners. Their positions on this matter are generally polarised, with trade unions arguing against forms of surveillance that interfere with workers' fundamental rights and negatively affect their working environment, and employer associations stating that monitoring in the workplace is necessary when carried out for legitimate purposes. In all countries, both trade unions and employer confederations routinely

provide their members with guidance with regard to employee monitoring and, in many cases, also legal advice.

In brief

- Technological advances have raised the bar for legislators and policymakers in the EU and added a new layer of complexity to the regulation of monitoring and surveillance in the workplace. National legislation struggles to keep pace with technological advances and often does not account, sufficiently or at all, for employers' use of state-of-the-art technologies for monitoring purposes. In only a handful of countries is the use of intrusive digital technologies in the workplace – such as biometric technology – addressed and regulated to some extent.
- In several countries, works councils or other workplace employee representatives have a certain influence over the introduction and/or use of technologies for monitoring in the workplace. Agreement or co-determination is required, for example, in Austria, Finland, Germany, the Netherlands and Sweden, while information and consultation is required in other countries such as Belgium, France and Romania. There are also instances of collective agreements at national intersectoral level, as found in Belgium and Norway.
- With the new EU General Data Protection Regulation (GDPR), data protection legislation has become a substantial element in the regulation of employee monitoring and surveillance in EU Member States. Although the GDPR contains some provisions relating directly to employment, the regulation of personal data processing in employment relationships falls within the remit of individual countries.
- National data protection authorities have an important role to play in enforcing existing rules and clarifying the relevant legislation by means of opinions, guidelines and recommendations. The implementation of the GDPR in national legislation has, in some cases, expanded the scope of activities of these public bodies.
- The international human rights framework has so far proven to be flexible enough to address some of the issues arising from technological developments, especially in relation to the protection of privacy, including in employment relationships, offering protection to individuals. Milestone judgments issued by the European Court of Human Rights (ECtHR) demonstrate that the protection granted by Article 8 of the European Convention on Human Rights extends to the workplace, that employees should receive adequate information on the scope and nature of surveillance and that the employer is required to justify the measures implemented and minimise surveillance by deploying the least intrusive methods. These judgments are particularly relevant for national lawmakers and jurisprudence in this area.
- The debate on employee monitoring and surveillance is typically framed by concerns about ethics, privacy and data protection. At a European level and in several Member States, trade unions have been particularly vocal in raising pressing concerns about potential infringements of workers' fundamental rights due to the use of advanced technologies in the workplace. In eastern European countries, monitoring and surveillance in the workplace is less of a subject of policy debate.

2 Scale of the phenomenon and new practices

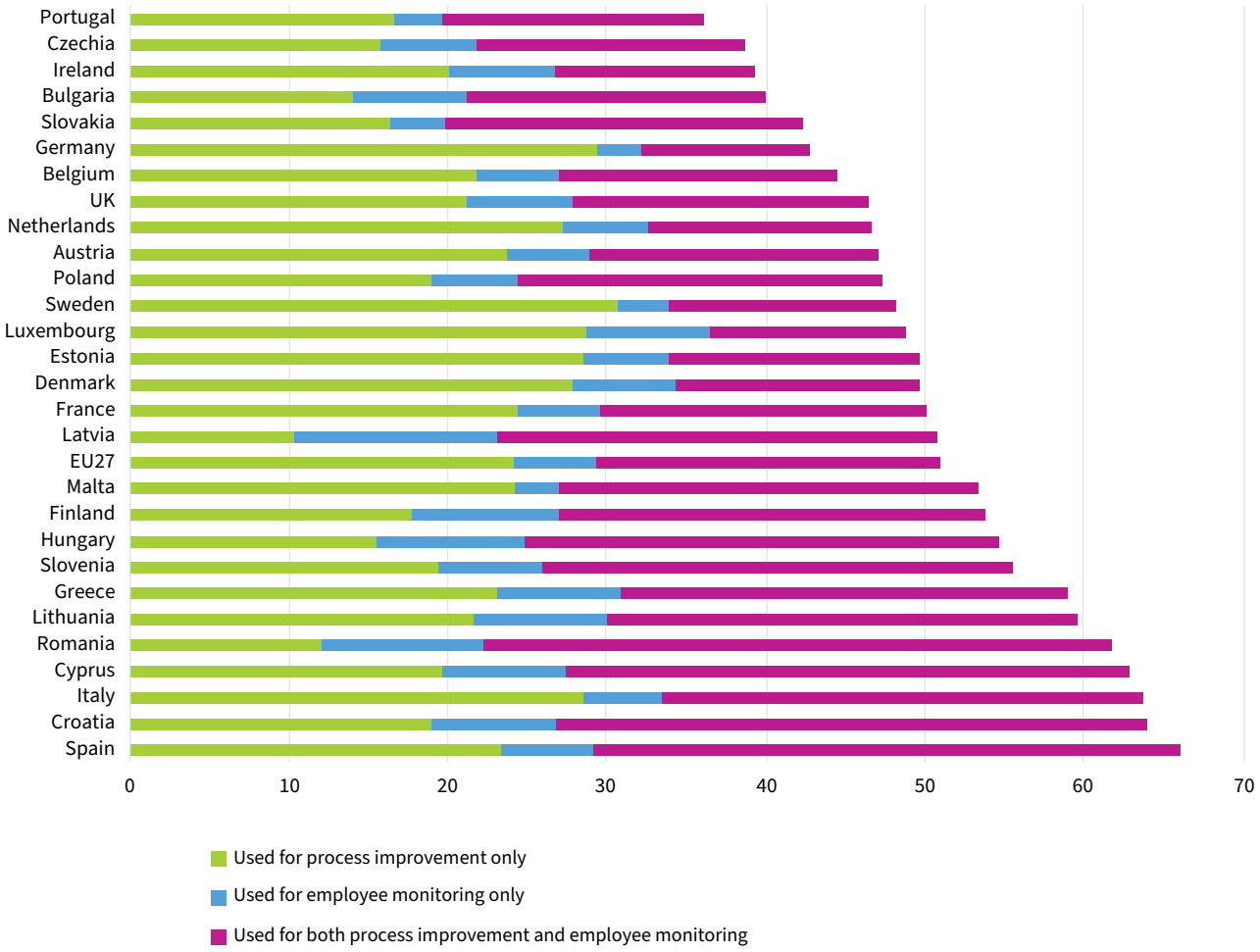
Extent of employee monitoring in the EU

European data

The fourth edition of the European Company Survey (ECS), which was conducted in 2019 in 21,869 establishments across the 27 EU Member States and the United Kingdom, provides some information on the use of data analytics for employee monitoring (Eurofound, 2020a).[10] In this survey, data analytics were defined as the use of digital tools for analysing the data collected within the establishment or from other sources. The managers surveyed were asked if data analytics were used in the establishment for the improvement of production processes and/or to monitor employee performance (Figure 1). The use of data analytics is also indicative of the use of algorithms to not only monitor but also assess employee performance.

Of the 51% of EU27 establishments reporting the use of data analytics, 24% reported their use for process improvement only, 5% reported their use for monitoring of employee performance only and 22% reported their use for both purposes. Therefore, data analytics, where used, tended to be used with the objective of improving processes more than for employee monitoring. Where establishments indicated that they had used data analytics

Figure 1: Use of data analytics for process improvement and/or monitoring employee performance, EU27 and the UK (%)



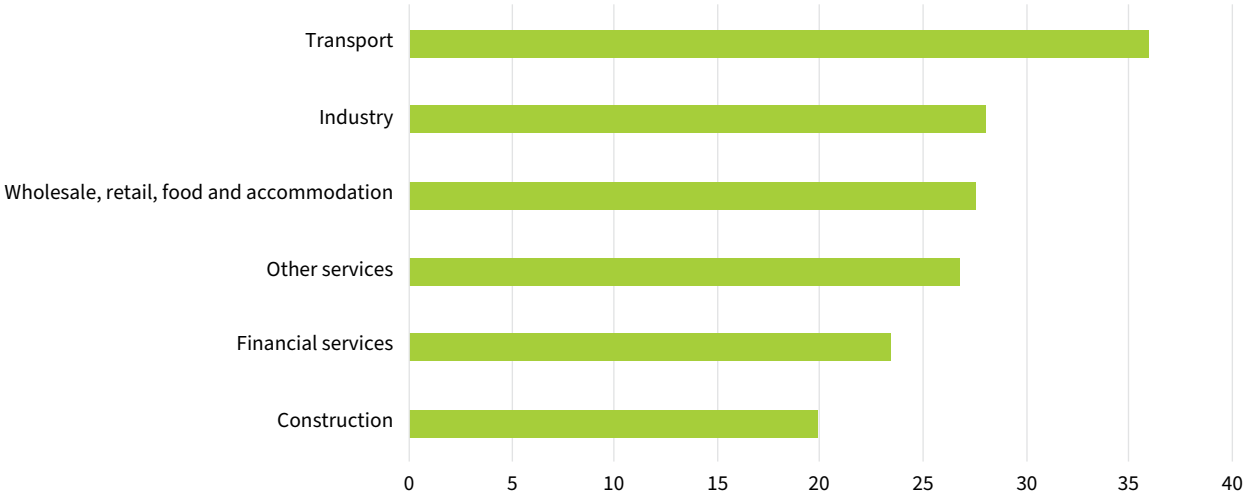
Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

10 The ECS 2019 was a cross-national survey. The target population was all establishments with 10 or more employees in economic sectors engaged in what are termed 'market activities' in all 27 EU Member States and the United Kingdom. Establishments across all EU Member States were contacted via telephone to identify a management respondent and, where possible, an employee representative respondent. Respondents were then asked to fill out the survey questionnaire online.

(for either purpose), their use had tended to increase in the previous three years. In 52% of establishments their use had increased, in 47% their use had stayed the same and in only 1% had the use of data analytics declined, according to management respondents. The use of data analytics for monitoring employees was reported most in Croatia (45%) and Romania (50%) and least in Germany (13%) and Sweden (17%).

In terms of sector distribution, the use of data analytics for monitoring employee performance is found to be most prevalent in transport (36%) and least prevalent in construction (20%) (Figure 2).

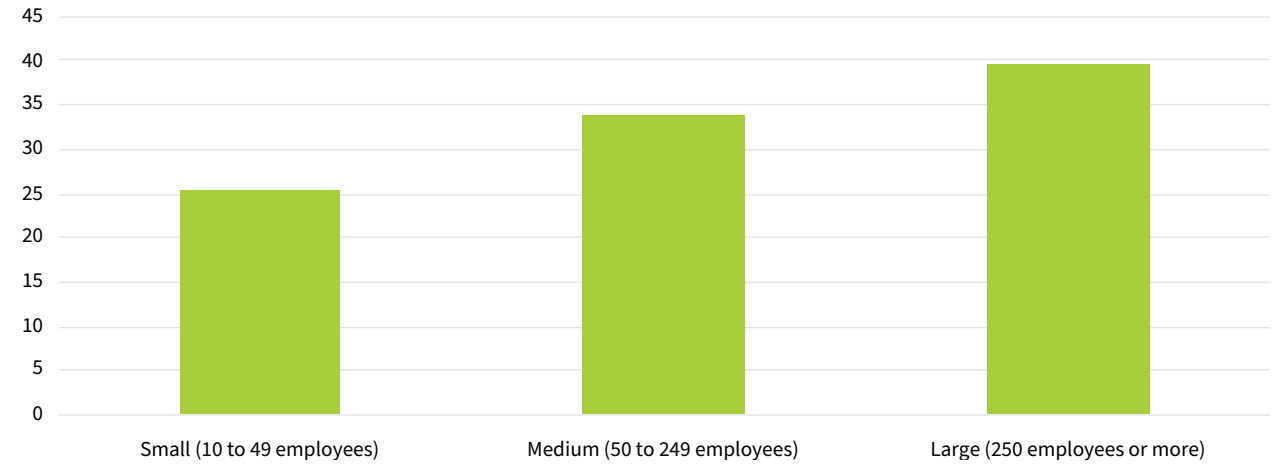
Figure 2: Use of data analytics to monitor employee performance by broad sector, EU27 and the UK (%)



Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

The use of data analytics for monitoring employee performance is positively correlated with establishment size (Figure 3). Large establishments (250 or more employees) were the most likely to report the use of data analytics for such a purpose and small establishments (10 to 49 employees) were the least likely (40% and 25%, respectively).

Figure 3: Use of data analytics to monitor employee performance by company size, EU27 and the UK (%)



Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

The survey also found that establishments with a recognised body for employee representation were more likely to report the use of data analytics to monitor employee performance (34%) than those with no formal employee representation (24%). This relationship weakens when controlling for establishment size but it remains significant, and it is unaffected by controlling for other factors, such as sector and country. At the same time, when such employee monitoring is in place, employees have a somewhat stronger role in influencing management decisions on the organisation and efficiency of work processes (Figure 4).

Figure 4: Use of data analytics to monitor employee performance by employee representation and influence over work process change, EU27 and the UK (%)

Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

National data

Only a handful of surveys have been carried out by national statistical offices or national research centres on employee monitoring or have touched on aspects related to this topic. The most notable example is the 2018 wave of the Finnish Quality of Work Life Survey (n = 4,110 people in employment aged 15–67 years) conducted by Statistics Finland.[11] To qualify as a respondent, a person had to work at least 10 hours per week. According to the survey, some 44% of survey respondents felt that the digitalisation of work had contributed to increased workplace monitoring. Nearly all of the employees surveyed stated that their work was monitored in one way or another, and only 7% said that they were not being monitored in any way. The most common way of monitoring was through recording the hours spent per task (57%), followed by performance-based monitoring (48%), access control (34%) and by means of software (17%) or cameras (13%). The method of surveillance was different for employees in different occupational positions. While 58% of upper-level white-collar employees said that their efficiency or work performance was monitored, this percentage was 45% among lower-level white-collar employees and 43% among blue-collar workers. Furthermore, among employees in less senior positions, monitoring by access control (39%), other technical equipment (11%) or cameras (19%) was more common than among employees in white-collar positions. For instance, only 29% of upper-level white-collar employees said that they were being monitored by access control and only 5% of them said that they were being monitored by camera surveillance. There were also differences between professional activities. In logistics, 32% of employees reported being monitored with the help of a monitoring device, and 28% of employees in customer service and/or in an office environment stated the same. In other sectors, the percentage was significantly smaller. Employees in retail (30%), security services (30%) and logistics (26%) were among those groups that were most often monitored with the help of a camera. In addition, differences between state, municipal and private sectors were also found. The use of access control, the recording of working hours, the use of software and the use of surveillance cameras were most common in the state sector, whereas among municipal employees these methods of surveillance were the least reported.

In this survey, the respondents were also asked if they felt that they had been monitored at their workplace even when nobody else was in sight. Among the respondents, 9% reported feeling this way often, while 24% said that they sometimes felt that they were being monitored. The employee's occupational position had an impact on how common this feeling was. Blue-collar employees and those in less senior positions felt this way more often than employees in the other two groups. Among blue-collar

11 Based on information published by Statistics Finland, 'the sample is obtained from the labour force survey by drawing from it either employed persons or wage and salary earners' (Statistics Finland, 2020).

employees, 14% reported feeling this way often (compared with 4% and 9%, respectively, among upper- and lower-level white-collar employees) and 40% reported feeling this way sometimes (compared with 22% and 36%, respectively, among upper- and lower-level white-collar employees).

An earlier and small-scale survey was conducted by the Finnish Institute of Occupational Health among top management within public and private organisations (*n* = 243) with more than 50 employees (Mamia et al, 2011). This study found that the use of electronic surveillance systems in Finnish workplaces was quite common; among such systems, the most reported were video surveillance systems (67%), monitoring of telephone calls (64%), electronic systems for monitoring expenses (65%) and working hours (63%), and monitoring of employees' internet usage (44%). There were also significant differences between sectors in terms of the extent and scope of electronic surveillance: it was most common in the service sector and least common in healthcare and education.

A nationally representative survey (*n* = 7,900 employees) on surveillance and monitoring of work was conducted by Statistics Norway (Bråten, 2016). This survey found significant differences between sectors, with monitoring of telephone calls prevalent in finance and insurance, and field technologies[12] more often used in sectors with mobile workers, such as in transport and warehouses, construction and utilities. Based on these results, Bråten (2016, 2017) conducted a survey of 1,463 employers in the four sectors with the most prevalent use of ICT-based surveillance and monitoring: manufacturing, finance and insurance, transport and warehouses, and public administration. The variation between the sectors is partly due to differences in the type of production and work tasks (Bråten, 2017). According to this survey, three out of four employers in the finance and insurance sector report using at least one of the monitoring and surveillance systems listed (Table 3). The use of camera surveillance and monitoring of telephone calls is highest in this sector. The use of monitoring and surveillance systems is also high in transport and warehouses, where field technologies are most used. In manufacturing, the electronic recording of work is most common.

Table 3: Prevalence of monitoring and surveillance systems reported by employers (%), Norway, 2016

System	Manufacturing (*n* = 540)	Transport and warehouses (*n* = 291)	Finance and insurance (*n* = 165)	Public administration (*n* = 467)
Total (at least one system)	30	57	74	36
Electronic recording of work	16	19	29	4
Field technologies	10	31	2	9
Camera surveillance	6	17	35	2
Monitoring of web pages	2	2	4	4
Monitoring of emails	4	6	21	20
Monitoring of telephone calls	2	6	30	6

Source: *Bråten (2017)*

This survey also found that the reasons most cited by employers for using monitoring systems were to comply with regulations or to ensure better organisation of work. To improve the safety of employees at work and for reasons related to customers or clients were also frequently mentioned as reasons for using monitoring systems. Motivations related to monitoring individual employees and their work were less frequently reported.

A more recent and comprehensive Norwegian survey on workplace monitoring and surveillance (*n* = 6,003 employees) was conducted by Fafo Institute for Labour and Social Research in 2019 (Bråten, 2019). It was designed to be as close as possible to the sample of the labour force surveys conducted by Statistics Norway and thus representative of the national workforce. The survey asked employees about the use of 11 such systems and whether they were used to monitor their work (Table 4).

12 Field technologies are defined as 'electronic systems or equipment designed to capture and communicate data on workers in the field so that employers can manage, document or inspect the behaviour and job performance of the mobile workforce' (Bråten and Tranvik, 2017). This includes GPS tracking, mobile positioning, electronic recording of driving, personal digital assistants, smartphone systems and related technologies.

Table 4: Prevalence of monitoring and surveillance systems reported by employees (%), Norway, 2019

Type of monitoring/surveillance	Use
Monitoring of telephone calls	8
Monitoring of the use of telephones/other communication technologies	9
Monitoring of emails	8
Monitoring of web pages	15
Monitoring of computer screen use (keylogging or screen capture)	7
Electronic recording of entry and exit	37
Camera surveillance of work areas	16
Field technologies	13
Biometric tools	8
Electronic recording of time use/productivity	25
Monitoring of internal chat rooms (Lynx, Facebook, Skype, etc.)	8

Source: *Bråten (2019)*

There were differences in terms of sectors when it comes to the use of various monitoring and surveillance systems. The most widespread use of such systems was found in finance and insurance, transport, warehouses, postal activities, and public administration (defence, police, tax and welfare authorities).

The survey also explored aspects of social dialogue and employee involvement. Some 40% of the employees surveyed reported that the use of monitoring and surveillance systems had been discussed with employee representatives, 15% reported that it had not and the other 45% of the respondents were unsure. Field technologies were the form of monitoring with the highest rate of reported dialogue (49%). In addition, 63% of respondents reported that their employer had informed them of the purpose of the monitoring, and 54% indicated that their employer had informed them about the use of the information gathered about them.

For Cyprus, data specifically on recording attendance and working time in the workplace are provided in the ad hoc module on work organisation and working time arrangements of the Labour Force Survey, covering employees and those who are self-employed (Statistical Service of Cyprus, 2019). About 54% of Cypriot employees reported that neither their presence at work nor their exact working hours were recorded, while 28% reported that their working hours were recorded automatically by a clocking system or at log-in. No information was provided, however, on the form of clocking system and whether this used biometrics or punch cards.

In France, some insight into the extent of use of employee monitoring is provided by the latest Medical Monitoring Survey of Professional Risks (SUMER) conducted by the Directorate of Research, Economic Studies and Statistics (DARES) of the Ministry of Labour. SUMER's main aim is to assess employees' exposure to harmful working conditions and to analyse appropriate protection mechanisms; it is not a survey specifically on employee monitoring and its impact on well-being, but provides information on the extent of monitoring via computer systems. The survey consists of interviews with employees conducted by company medical officers during their regular compulsory medical examination. The 2017 edition of the survey covered 26,500 employees in the private and public sectors. The survey's findings show that monitoring via computer systems had increased steadily between 1994 and 2017 (+18 points), with almost a third of employees monitored in this way in 2017. According to DARES (2019), this trend reflects the decrease in middle management and the spread of digital tools.

On the specific issue of data protection, the AP published a survey (n = 1,002 residents in the Netherlands) in 2019, which found that 94% of the Dutch population is worried about the protection of their personal data. Regarding the question on which organisations the Dutch are most worried about, 'their employers' was among the top six categories, after technology companies, the government, banks and insurance companies, pension funds and healthcare institutions.

Box 1: Studies on employee monitoring by trade unions and professional associations

There are only a few surveys and studies on employee monitoring – found in this research – that were commissioned or conducted by trade unions and professional associations. In the UK, the TUC commissioned qualitative and quantitative research on workplace monitoring and surveillance. The qualitative stage of the research involved a range of focus groups and in-depth interviews held across four cities (London, Birmingham, Manchester and Bristol). The results of these interviews were used to develop a follow-up online survey carried out in May 2018, which received 2,100 responses from members of the UK public; the results were weighted to be representative of the UK adult population (TUC, 2018). Questions relating to an individual's specific workplace or current experiences of work were addressed only to those in work at the time of the survey. The survey found that 56% of workers believed it was likely that they were already being monitored at work. Monitoring appears to be more common in large companies. According to the survey respondents, the most common forms of employee monitoring include monitoring employees' work emails, files and browsing histories, CCTV, and telephone logs and calls, including the recording of calls, but more advanced forms of monitoring (such as facial recognition and handheld/wearable location-tracking devices) are gaining traction. Among the workers surveyed, 70% expected workplace monitoring to become more widespread in the future and had concerns in this regard. Around three-quarters of respondents (76%) considered the use of facial recognition software and

monitoring of employees' social media usage outside working hours to be unacceptable. While the survey found that 79% of respondents believed that employers should be legally required to consult employees before the introduction and implementation of any new form of monitoring in the workplace, over 80% said that employers should be obliged to provide a clear and understandable justification to their workforce for the introduction of a new form of workplace monitoring.

In 2018, the Central Organisation of Finnish Trade Unions (SAK) conducted a survey among its blue-collar union members (n = 1,202) on the digitalisation of work, which also touched on the issue of employee monitoring (SAK, 2018). A quarter of the interviewees said that some kind of technical device or program was used to monitor their performance at work. Nearly half (48%) of the respondents agreed or strongly agreed with the statement that new technology has increased the surveillance and monitoring of their work, while 18% disagreed and 35% strongly disagreed with this statement.

A qualitative explorative study on workplace surveillance was conducted in 2016 by the Swedish Confederation of Professional Associations (SACO, 2016). The employers and local trade union representatives interviewed (n = 20) reported that electronic surveillance was common in Swedish workplaces in one form or another. Most of the interviewees stated that employees' search histories were saved and, in some cases, also monitored. Video surveillance systems were reported to be widely used; the interviewees considered that video surveillance was acceptable if it was installed for security reasons. Interviewees also reported being aware of email correspondence being monitored for security reasons, but also for monitoring employee performance. A few interviewees reported that employees' computer and telephone usage was also monitored, with the data collected being used in personal development meetings and to support pay negotiations.

There are also instances of studies that were carried out by sectoral trade unions. For example, the Danish Union of Public Employees (FOA) conducted a survey that found that one in six employees (18%) in the social and health sector had experienced being monitored during working hours (FOA, 2018). Of the employees who reported having been monitored by means of video surveillance, over half (61%) stated that they perceived it as an infringement and that surveillance did not serve an important professional purpose or make them feel safer. In addition, in 2015, the Danish Union of Commercial and Clerical Employees (HK Handel) conducted a survey among its members. About 12% of respondents reported that video surveillance was used in their workplace to monitor employees' work performance. Some 14% stated that video surveillance at the workplace created uncertainty, and another 15% believed that being monitored was a source of stress (Fyens Stiftstidende, 2019).

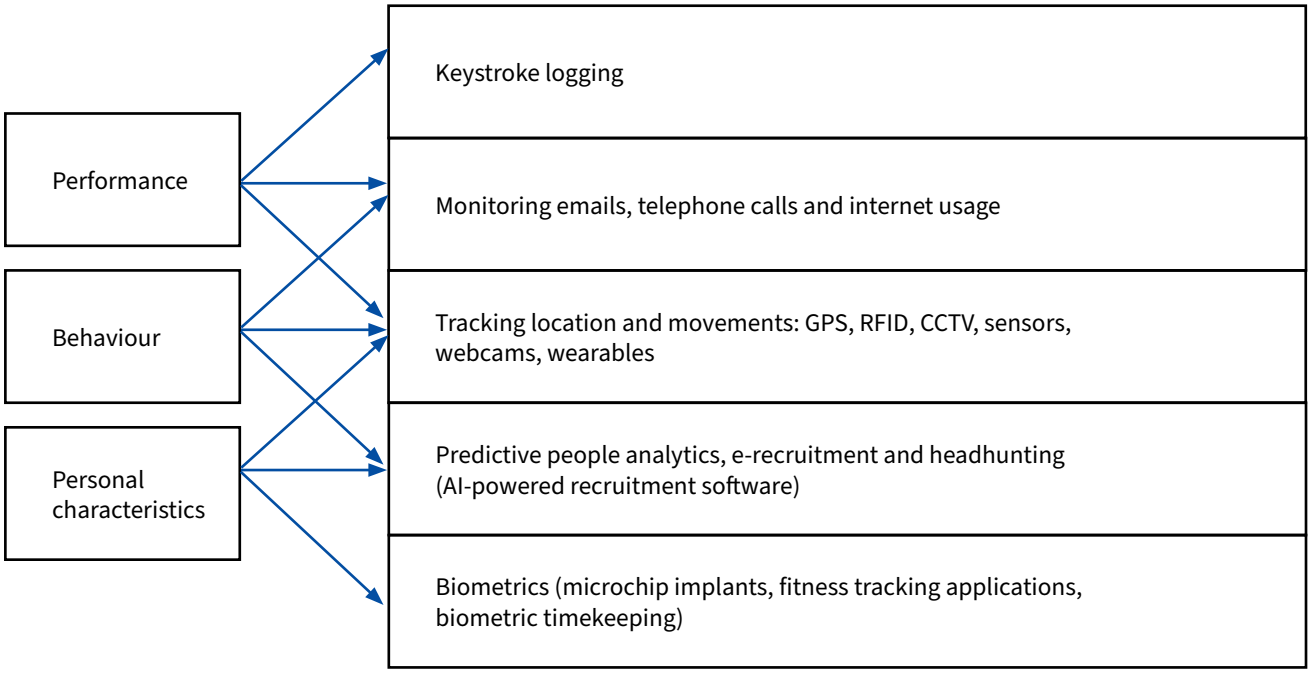
More specifically on the topic of remote working, a survey (n = 2,224 employees in the UK) commissioned by the UK Chartered Institute of Personnel and Development (CIPD) and carried out in 2016 found that a fifth of the employees surveyed thought that 'remote access to the workplace' (through work devices, mobile technology, video and other methods) made them feel 'as though they are under surveillance' (CIPD, 2017).

New digital-based monitoring and surveillance practices

Technological advances have broadened employee monitoring capabilities beyond the more conventional forms of monitoring in the workplace, such as CCTV surveillance and monitoring of emails, telephone calls and internet usage.

Surveillance techniques and devices – enhanced by digital technologies – can be used to monitor employee performance, behaviour and/or personal characteristics (Figure 5) and have the potential to become central to work management systems.

Figure 5: Techniques and devices for employee monitoring and surveillance



Source: *Adapted from Ball (2010)*

There is some evidence that the recent COVID-19 pandemic has accelerated the uptake of new digital devices for employee monitoring. The need for remote work during the crisis has, for example, created a new market for keylogger software to monitor the computer-based activities of employees working remotely and other software that takes webcam shots of employees at regular intervals and thereby monitors their availability and presence in front of their computer (Business Insider, 2020; The Washington Post, 2020).[13] According to Google trends, the use of the search term 'remote employee monitoring' peaked around the beginning of the COVID-19 lockdown in spring 2020. With remote work becoming more mainstream, it is likely that companies will invest more in technologies for tracking employee performance (Sostero et al, 2020).

Albeit often framed in a negative way, the use of digital technologies for employee monitoring can be justified by the nature of the activity performed and can have some benefits for workers. However, it may be difficult to disentangle legitimate reasons from privacy intrusions or even infringements. For example, GPS tracking, which has been used for some time by transport and delivery firms, can provide workers with information that eases their work, but it also opens the door to intrusive employee performance monitoring, including tracking the length of rest breaks and out-of-work movements.

Monitoring performance and behaviour

Wearable technology – such as smartwatches, smart bracelets and smart glasses with in-built GPS capabilities and sensors tracking movements and location and counting steps and pulses – is an emerging trend in the workplace. According to consulting firm Deloitte (2018), advances in enabling technologies are driving enterprise adoption of wearables. In 2018, American consumer electronics and fitness company Fitbit – recently acquired by Google – launched Fitbit Care, a platform aimed at employer wellness programmes (Business Insider, 2018). Fitbit-like devices generate a constant stream of personal data, which are fed directly or indirectly to third-party firms including insurance companies and may, for instance, be used to adjust health insurance premia based on personal health data or behaviour. This practice is most common in the United States, but technology companies are also entering the healthcare industry in Europe, with potentially disruptive effects (Financial Times, 2020).

There are many instances of controversy being sparked by wearable devices being used for employee monitoring, which have been reported in the media over the years. One such instance is the handheld scanner used in Amazon's warehouses ostensibly to record task completion and to coordinate work organisation. Their use can, however, be less benign, as they can also be used to monitor employees' performance (miles walked, objects delivered or packed) in relation to production targets, including keeping track of toilet breaks. According to a UK survey carried out by worker rights platform Organise, 74% of the Amazon workers surveyed avoided using the toilet for fear of receiving warnings for missing performance targets, and 55% reported having suffered depression since working at Amazon (Organise, 2018).

This Amazon monitoring practice has been condemned in Poland by trade union NSZZ Solidarność, which has highlighted the fact that employees in Amazon fulfilment

13 One such web-based application that attracted publicity during the lockdown was the aptly named sneek.io, which offers employers and employees a window on their fellow employees' presence in front of their computers by taking webcam shots up to every half-minute.

centres in Poland experience less favourable working conditions than their counterparts in Germany and the UK (Wiadomosci Handlowe, 2019). Owczarek and Chełstowska (2016) also observe that the work organisation in Amazon is 'based on Taylorist ideas supplemented by meticulous electronic measurements' (p. 22).

In a 2020 report, Hanley and Hubbard discussed Amazon's surveillance infrastructure, which encompasses an extensive network of security cameras installed in warehouses that track workers' movements, item scanners that monitor individual performance and navigation software that monitors routes for delivery drivers. According to the authors, such surveillance practices should be prohibited outright, as they dehumanise work and intensify precarity, curtail workers' autonomy and individual decision-making, and harm workers' physical and mental health (Hanley and Hubbard, 2020).

Amazon is well known for its in-house experiments before selling new technologies widely. In 2018, the retailer was said to have patented the design for ultrasonic wristbands that replaced the handheld scanner and potentially enabled more intrusive monitoring of warehouse employees (The Guardian, 2018b; The New York Times, 2018). The retailer also filed a patent for a pair of augmented reality goggles that showed employees where to place objects. These technologies, however, raise privacy concerns, as they can potentially be used to enhance employee monitoring (The Telegraph, 2018). More recently, faced with criticisms for failing to protect workers from COVID-19, Amazon has announced the deployment of an AI 'distance assistant' to track employees' movements in real time and remind workers of social distancing guidelines (The Verge, 2020). Again, the fear is that such a device can be also used for employee monitoring purposes.

Following well-established surveillance practices at Amazon, the UK-based multinational grocery store chain Tesco also made it obligatory for warehouse workers and forklift operators in Dublin's distribution centres to wear Motorola arm-mounted terminals for monitoring their productivity. This monitoring practice was, however, discontinued shortly after it was introduced in 2013 owing to negative publicity (Irish Independent, 2013).

Wearable technology can, however, be used for the benefit of workers, to keep them safer. For example, in the UK, Oxfordshire County Council announced in 2018 that it would provide waste recycling teams with body cameras to keep staff safe and discourage physical and verbal abuse from the public (Oxfordshire County Council, 2018). Wearables are also offered by employers as part of corporate well-being programmes to encourage employees to stay fitter and heathier (and presumably more productive). According to a survey conducted by PwC (2016), 61% of the employees surveyed reported being keen for their employer to take an active role in their health and well-being. The use of such wearables provided by employers for personal purposes may, however, lead not necessarily to greater employee well-being but rather to an increasing enmeshing of employees' private and work lives and merging of personal with work-related data, with implications for both employees and employers.

Employees may not be aware of the trail of data that they leave behind and they may not realise, at least initially, that they give away personal information to their employer or third parties. A case study from the Dutch literature (Rimmelzwaan, 2017) also shows that the perceptions and attitudes of employees change in relation to the use of wearables provided by the employer as they give more consideration to and become more aware of data usage issues. In this Dutch case study, an SME operating in the ICT sector initiated the use of a wearable device to promote well-being and health behaviours among its employees. Although employees were initially enthusiastic about the use of the wearable device, they later indicated that it did not lead to a sustainable behavioural change and their appreciation of the device changed as they became more concerned about data usage.

Tracking devices also exist that use sensors to monitor employees' movements and activity in the office. For example, Barclays has been using a staff monitoring scheme at its London headquarters, which uses tracking software to log the time that employees spend at their desks and monitor the length of toilet breaks. The system also makes suggestions to employees falling behind targets. The TUC condemned the practice as 'dystopian Big Brother tactics that show a total disregard for hardworking staff' (The Guardian, 2020). In 2017, Barclays had already been harshly criticised for the use of a tracking device called OccupEye, which used heat and motion sensors to record the time spent by employees at their desk. In a statement, Barclays clarified that the intention was not to monitor employees' productivity but to assess office space usage and improve energy efficiency (Independent, 2017). A similar sensor-based tracking system was introduced in 2016 at the Daily Telegraph offices in the UK to monitor how long employees were at their desk, but its use was discontinued following harsh criticisms by the National Union of Journalists, which accused the newspaper of 'Big Brother-style surveillance' (The Guardian, 2016).

More extreme is the use of microchip implants. Although this is not yet a common practice in the EU, it nonetheless hit the headlines in the UK when human microchipping companies were said to have already fitted implants or to be in talks with a number of employers about microchip fitting (The Guardian, 2018a). In addition, in Estonia, known for being a leader in digital society implementation, the telecommunications operator Tele2 had chip implants fitted under the skin of some of their employees, who had volunteered to be chipped (NFC World, 2018). The reported benefit of these chip implants was that staff could pass through company authorisation systems without keycards, but this technology could potentially be used for more pervasive and intrusive employee monitoring. Microchip implants are also becoming very popular in Sweden, especially in a bid to reduce the spread of the COVID-19 virus by eliminating the need for credit cards, cash and keycards to access offices and buildings (EuroWeekly, 2020). The use of these implants, however, raises issues

around, among other things, data ownership, sharing and integration with other systems.

Monitoring personal characteristics

Equally controversial is the use of biometric devices for workplace monitoring, especially for working time recording and attendance control. The general approach in the EU is that the data generated through methods such as facial and voice recognition as well as via fingerprints and retinal imaging can be used only in exceptional circumstances. Technology is developing at a rapid pace and the progression from facial recognition technology to emotion recognition technology is happening fast. Such technology could potentially change recruitment practices. Machine-learning algorithms can detect the emotional expressions of job applicants, matching them with personality traits and, in doing so, can help to screen out prospective applicants with undesirable characteristics. This technology is already being used in recruitment by global consumer goods manufacturer Unilever (Forbes, 2018). If misused, AI-based systems can result in serious infringements of workers' rights and dignity and not least in unfair and discriminatory employment decisions. For instance, Amazon attracted negative publicity in 2018 when its Edinburgh engineering hub was found to be using AI software to sort job applications, with the lexical analysis of CVs favouring words more commonly used by male applicants, thus discriminating against women (Reuters, 2018). Predictive people analytics tools and data-mining techniques are also used by some employers – for example, CreditSuisse and Wal-Mart – to make predictions about employees' future behaviour and to estimate staff turnover (Business Insider, 2014; The Wall Street Journal, 2015).

The use of emotion recognition algorithms has been criticised by UNI Global Union in relation to a case in which an AI system was used to assess the tone of voice and mood of call centre workers in dealing with customers, with those data then used in appraisals (Prospect, 2020). A host of new privacy issues also arise from the use of these algorithms: for example, if and to what extent GDPR legislation applies to data from AI-powered technology. According to a recent legal analysis by Berlin-based non-governmental organisation AlgorithmWatch (2020), although employers need to obtain individual consent from each employee before running AI-powered data analytics systems, they rarely do so, thus breaching the law, often without being aware of it. A survey conducted in 2020 in the UK by the trade union Prospect among its members (n = 7,750) shows that almost half of them (48%) reported not being confident or being not confident at all that they knew what data their employer collected about them at work. In addition, over 70% had no confidence in their employer to involve them in decisions about how new technology would be implemented.

Albeit often contested and debated, biometric technology is slowly but surely entering the world of work. Public attitudes towards biometric devices may already be changing as facial recognition and other touchless biometric-based systems – for example, for clocking in and out or accessing company premises – could be seen as more effective in limiting, for example, the spread of COVID-19. The risk is that employees become habituated to these new devices as they are introduced initially for purposes other than performance monitoring. Then, once they are implemented in the workplace and their use is legitimised, it is more difficult to stop using them.

In brief

- Based on data from the European Company Survey 2019, around half of establishments in the EU27 and the UK use data analytics for process improvement, for monitoring employees or for both. This percentage breaks down as follows: 24% use data analytics for process improvement only, 5% use data analytics for monitoring employee performance only and 22% use data analytics for both purposes. Large establishments (with 250 employees or more) are more likely to use data analytics for monitoring employee performance than smaller ones. This use of data analytics is positively correlated with the presence of a recognised body for employee representation in the establishment. This holds true when controlling for establishment size, sector and country.
- There is limited empirical evidence on the extent of employee monitoring in individual countries; to date, there are very few national surveys touching on aspects related to this topic. The most notable examples of large-scale surveys are found in Finland and Norway, suggesting that the use of electronic monitoring systems is a common practice in those countries, with more advanced forms of monitoring gaining traction. In some countries, notably in the UK and the Nordic countries, trade union organisations and professional associations have sponsored or conducted surveys exploring employees' concerns in relation to monitoring and surveillance in the workplace. Among employees' main concerns are the invasion of privacy enabled by the use of digital technologies for employee monitoring purposes and the lack of transparency vis-à-vis the nature and content of the monitoring.
- In addition to national data from surveys, anecdotal evidence indicates that more intrusive monitoring and surveillance practices, enabled by advanced technologies, are making their way into the workplace. The use of digitally enabled employee monitoring has expanded the possibilities for monitoring employees' performance and behaviour, with greater possibilities to factor in employees' personal characteristics as part of the monitoring. The use of algorithms, data and AI for evidence-based work management, human resources and recruitment also opens avenues for discrimination and may result in unfair employment decisions.

3 Implications for job quality

Key considerations

A number of researchers argue that new forms of monitoring and means of surveillance – enabled by new digital technologies – may have serious negative impacts on workers' privacy, dignity and autonomy, particularly in the case of misuse (Moreira, 2016; Canteiro, 2017; Azevedo, 2018). Oliver (2002) asserts that privacy-invasive monitoring practices can also inhibit creative thinking, limit independence of thought and induce stress-related illness.

The Spanish Strategy for Health and Safety at Work 2015–2020 emphasises the need to be mindful of the potential impact of the use of new technologies on workers' health and safety (INSHT, 2015). The strategy points to the increasing and more pervasive use of ICT that facilitates the use of worker surveillance programs to ensure accountability, particularly in the context of remote working and other flexible working arrangements.

Some recent research studies look at the negative effects of employee monitoring technologies that adopt work management functions, with workers being provided with suggestions or directions based on their actions in real time and given performance scores (or other forms of benchmark) (Mateescu and Nguyen, 2019). This leads to the 'gamification' of work, which can result in a high-pressure and competitive work environment, and can potentially weaken the organising and negotiating power of workers, devaluing the (monetary) value of work (Casilli, 2019). Workplace gamification is, however, not inherently negative: if well established, it can promote employee engagement, innovation and learning at the workplace (Forbes, 2017). Concerns arise when gamification is used in combination with pervasive digitally enabled employee monitoring and in the context of technologies that are increasingly taking on management functions.

Zuboff (2019) argues that the very fact of being under surveillance changes the behaviour of those being watched, curtailing their autonomy and infringing on their privacy. Surveillance in the workplace is no exception. The constraints on autonomy engendered by intrusive employee monitoring and surveillance practices risk undermining the psychological contract between employee and employer,[14] reducing employees' trust, motivation and commitment to the organisation (McParland and Connolly, 2019). This is particularly the case if there is no transparency in relation to the monitoring methods and the use made of the data collected. Previous research on employees' perceptions of electronic monitoring in the context of the psychological contract indicates that electronic performance monitoring is perceived as an unfair practice, a violation of privacy and a breach of the psychological contract (Tabak and Smith, 2005; Chory et al, 2016). As a result of this, employees become less committed to the organisation and withhold effort, hence defeating the whole purpose of employee monitoring – to enhance performance – and becoming counterproductive.

Monitoring of mobile and remote workers

Company case studies produced by Eurofound in the framework of research on teleworking and ICT-based mobile work[15] suggest that the use of digital technologies has enhanced the potential for remote workers to be controlled and/or monitored and that works councils or other forms of employee representation have an important role to play in setting boundaries to the use of intrusive technologies for employee monitoring (Eurofound, 2020d).

14 The notion of the psychological contract refers to the employee's set of beliefs and expectations of mutual obligations that link employees and employers (Rousseau, 1995). Trust and fairness are core elements of the psychological contract (Tabak and Smith, 2005).

15 Eurofound defines teleworking and ICT-based mobile work as follows: 'Telework and ICT-based mobile work (TICTM) is any type of work arrangement where workers work remotely, away from an employer's premises or fixed location, using digital technologies such as networks, laptops, mobile phones and the internet' (Eurofound, 2020a).

Box 2: Case study evidence on digital surveillance in teleworking and ICT-based mobile work

Both management and the works council representative in a German ICT company shared the view that digitalisation enabled constant traceability of the information flow between sales agents and business clients. As part of an ICT upgrade, sales agents were required to record each step of their project through a smartphone or digital notebook, which, at least in principle, made it possible for management to monitor employee performance. Although the works council opposed the use of data analytics for monitoring performance, it was technically feasible to use this technology to monitor employee performance.

In another case study from the Spanish wholesale and distribution sector, handheld devices with geolocation features were used by managers and supervisors to monitor and track salespersons' schedules and routes. According to both trade union and management representatives, the use of these devices had both improved performance and increased organisational control. The handheld devices recorded relevant information, which was used to estimate the total working hours for each salesperson by line managers. Managers and supervisors used the working time information gathered through the ICT devices to put pressure on employees. The trade union representative felt that the information collected was biased and inaccurate, as it did not take into account activities that were inherent to the work carried out by the employees (for example, commuting and loading goods). In addition, the monitoring was extended to other areas that were previously left to employees' own discretion, such as route planning for visiting clients in a working day.

In another Spanish case from the banking sector, although ICT resources were available that could be used to monitor work done remotely, managers paid more attention to the fulfilment of objectives than to the actual time spent on the execution of tasks. The trade union representative in this case study noted that, in departments where working to tight deadlines prevailed, it was difficult for an employee to 'pretend to be working' and close monitoring would be counterproductive. In addition, the corporate policy aimed to prevent managers from acting in ways that could undermine the autonomy of employees working remotely.

Source: *Eurofound (2020d)*

Qualitative research carried out among London bus drivers using semi-structured interviews gives an insight into the use and acceptance among mobile workers of monitoring and control systems (Pritchard et al, 2015). The drivers used an on-board performance monitoring device known as Drivewell, which calculates a performance score for each driver based on various recordable driving behaviours. If the score attained is poor, the driver is sanctioned or forced to undertake some training. This device was perceived by drivers as a form of management control; the feeling of being watched changed their driving behaviour and, according to some drivers, gave rise to a competitive culture.

The research also suggests that such systems place additional demands on drivers' attention, adding to the range of other surveillance technologies and driving distractors, potentially increasing stress. Although some drivers reported using the device as a learning tool and an opportunity to improve their driving, the accuracy of the performance scores was challenged by some drivers, as the system failed to take into account the quality of the vehicle used and the nature of the roads driven on. The general consensus among drivers was that the technology did not fully measure their skills or job performance and instead had the potential to limit their discretion and possibly their future prospects.

Another qualitative research study on the impact of remote monitoring (using field technologies to monitor the behaviour and performance of mobile workers) conducted in 52 private companies and public organisations in Norway found that employee representatives who felt that field technologies threatened workers' privacy also tended to report negative effects on job quality (Bråten and Tranvik, 2017). Such views were most prevalent in industries where field technologies were used to direct and control work, especially in the transport of goods and the installation of electronics and energy supply. Where the use of field technologies was motivated by the need to document or inspect the work done, negative views were less prevalent. Commonly cited concerns were less individual freedom and reduced influence over one's work day and work tasks, as well as an increase in stress, work pace and pressure. Another reported concern was that many employees were unsure about what use the employer would make of the information gathered about them. Employee representatives in the roadworks, security and nursing home sectors also reported similar concerns, but some positive effects noted were increased security – for example, as a result of being able to quickly call for help in emergencies – and an enhanced ability to document work and thus refute potential complaints. One negative impact, reported across most sectors, was increased conflict and less trust between the social partners following the implementation of field technologies. In some companies, trust was restored after some time, while in other companies this did not happen because the technology was seen as indicative of mistrust in individual workers.

Employees' attitudes and perceived impact of monitoring

Current research suggests that the use of electronic performance monitoring without a clear purpose is likely

to produce negative attitudes and is counterproductive for the organisation, as it ultimately undermines the performance of those being monitored (Ravid et al, 2019).

Employees' attitudes to monitoring in the workplace are not, however, necessarily all negative. A small-scale Finnish qualitative research study (Keyriläinen and Sutela, 2018) found that some employees perceived the requirements to record different aspects of their work as contributing to transparency, while for others it was a form of control and surveillance.

In addition, findings from a Norwegian survey (Bråten, 2019) conducted among a representative sample of 6,003 employees indicate that many respondents do not view workplace monitoring negatively: in fact, most did not fully agree with the negative statements formulated in the survey with regard to the effects of different forms of monitoring implemented at their workplace (Table 5).

Table 5: Proportion of employees agreeing with statements about monitoring measures in the workplace, Norway, 2019 (%)

Statements	Monitoring of communication (*n* = 870)	Access control (*n* = 1,249)	Camera surveillance (*n* = 408)	Monitoring of work/performance (*n* = 937)
Provides safety in my relations with clients, customers, users, etc.	47	37	71	33
Is necessary for the employer to be in control of time use and productivity	22	22	12	47
Makes me afraid to commit errors at work	18	6	14	12
Is a source of stress when conducting my work	21	9	16	22
Gives the employer too much control over how I do my work	29	13	19	27
Is important as a part of the training to do the work satisfactorily	24	13	15	21
Gives me less flexibility in my working day	23	12	14	20
Gives my employer the opportunity to also monitor what I do in my spare time	25	9	13	11
Contributes to diminishing trust between management and myself	25	13	15	19
Contributes to diminishing trust between myself and colleagues	14	8	11	10
Contributes to diminishing trust between myself and customers, clients, students, etc.	12	7	9	7
I feel uncomfortable with this	29	11	17	19
Affects job satisfaction and work environment negatively	23	12	15	20

Notes: *Cell percentages represent the proportion of respondents who fully or partly agreed (scored a 4 or 5 on a 5-point scale) with each statement. The percentage in each cell is calculated from the subset of respondents who previously reported that a given control measure was implemented at their workplace. Only this subset was asked whether they agreed or disagreed with the statements (for example, 1,249 out of the 6,003 respondents reported there was access control at their workplace and these respondents were then asked whether they agreed or disagreed with the statements in relation to access control systems). Finally, each category is composed of several concrete measures. 'Access control' includes electronic recording of access, log-in systems and biometrics.*

Source: *Bråten (2019)*

A significant minority of respondents, however, reported some perceived negative effects across the four forms of workplace monitoring. Monitoring of communication seems to have the greatest impact on job quality, as respondents with these systems tended to agree with the negative statements more often than those who were subject to other forms of monitoring. Monitoring of work and performance had the next greatest impact, as often it was seen as necessary but also as a source of stress. Camera surveillance was seen by most to provide safety in the workplace. Access control generally seems to have less impact on the work environment, possibly because it does not involve constant monitoring and may be perceived as less intrusive.

From a more qualitative research perspective, a small-scale study (Garzia, 2013) conducted in Malta explored perceptions of electronic monitoring among employees in government entities and the possible outcomes associated with technological surveillance. In this study, 'electronic monitoring' referred to practices not directly related to performance and included biometric-based time attendance systems (also referred to as 'palm readers'),

as well as telephone monitoring and a variety of computer-aided monitoring systems such as email and internet monitoring. The study participants did not criticise the use of the technology as such, but rather the way in which the organisation managed monitoring systems, which at times was perceived as being unjust. The participants reported a range of feelings and emotions in relation to the experience of being monitored, namely discomfort, frustration and vulnerability, which had an impact on their well-being. The findings also suggest that electronic monitoring had a detrimental impact on the management–employee relationship, as it may be construed as a sign of mistrust. Trust issues seem to have been exacerbated by management's lack of communication vis-à-vis the introduction and implementation of monitoring systems.

Attitudes towards monitoring in the workplace may also be influenced by cultural norms and the general level of trust in society. For example, a Swedish survey that was representative of the national population (n = 1,118) suggests that attitudes towards surveillance in Swedish workplaces tend to be rather permissive (Rosengren and Ottosson, 2016). Only 20% of the respondents agreed with the statement that camera surveillance is a potential threat to personal integrity. Half of the respondents (50%) did not know what type of information employers were gathering on their internet use. Only 21% agreed with the statement 'I worry that my employer will monitor my use of internet and email', while 56% disagreed.

Another survey-based study carried out in the UK (n = 425) explored employees' attitudes to workplace surveillance using a 16-item surveillance-at-work measure and correlations with autonomy, job satisfaction, attitudes to authority and perceived discrimination at work (Furnham and Swami, 2015). The research shows that those who are more negative about workplace surveillance also report experiencing less autonomy at work. Negative attitudes to workplace surveillance were also correlated with lower job satisfaction, more negative attitudes to authority and greater perceived discrimination at work. The opposite was found to be true for positive attitudes to workplace surveillance.

Experimental studies on electronic performance monitoring

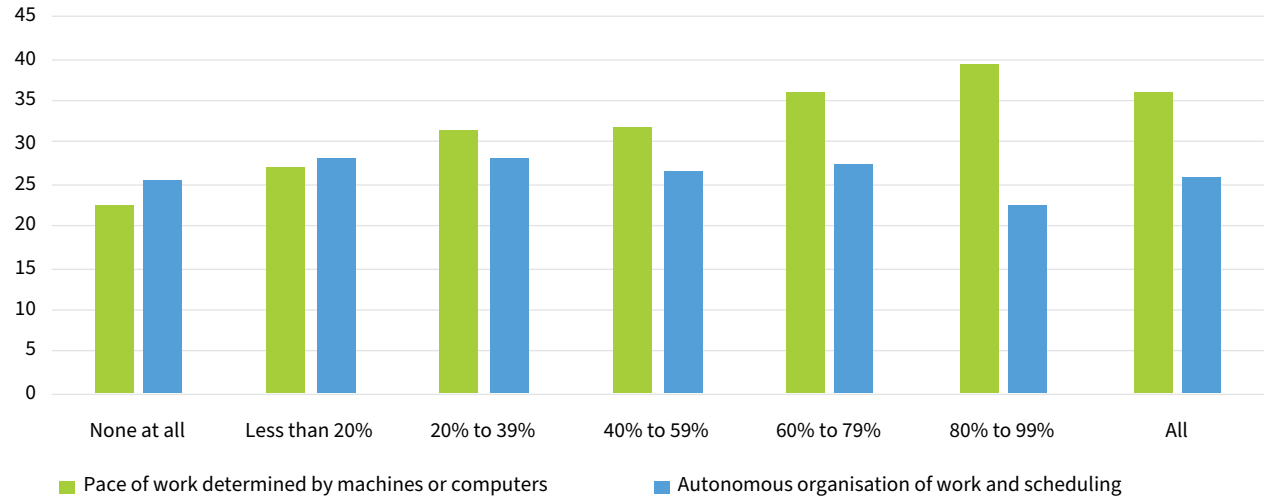
A number of experimental studies looked into the effects of electronic monitoring on task performance (see Ravid et al, 2019, for a review); however, these have produced no conclusive evidence on whether or not those who are electronically monitored perform better than those who are not. When electronic performance monitoring was found to be effective at increasing performance levels in relation to a task, it was at the expense of other tasks not being monitored. Counterintuitive findings come from a French experiment (Gillet et al, 2016) conducted in a call centre using electronic performance monitoring systems, which found that a reduced intensity of electronic monitoring resulted in a slight increase in performance but an unexpected deterioration of aspects of job quality (measured via a standardised test). This was explained by the researchers as due to the loss of real-time access to performance indicators, which may give call centre workers a sense of control over their work, and supervisors exerting other forms of intrusive surveillance that compensated for the reduced level of remote monitoring.

Use of data analytics to monitor employee performance

The ECS 2019 offers insight into the correlations between the use of data analytics for monitoring employee performance and work organisation practices (Eurofound, 2020a). For example, to assess the level of autonomy that workers have within the workplace, the survey asked managers about the proportion of the employees in their establishment who organise their tasks and their time independently and whose pace of work is determined by machines or computers.

Each category depicted in Figure 6 represents the proportion of employees affected by a specific work organisation modality according to the management representatives surveyed who reported that their organisation uses data analytics to monitor employee performance. One could hypothesise that such monitoring would be useful to employers with a high proportion of employees working with a high degree of individual autonomy. However, this appears not to be the case; there is little obvious relationship between the proportion of autonomous workers and the incidence of employee monitoring. There is, however, a somewhat stronger correlation between the existence of such monitoring and workplaces where the pace of work is significantly determined by machines or computers. This suggests that employee monitoring data may emanate directly from such technological processes of production. Nonetheless, even in workplaces where the pace of work is highly determined by machines or computers (80% or more), just a minority (36–39%) report the use of data analytics to monitor employee performance.

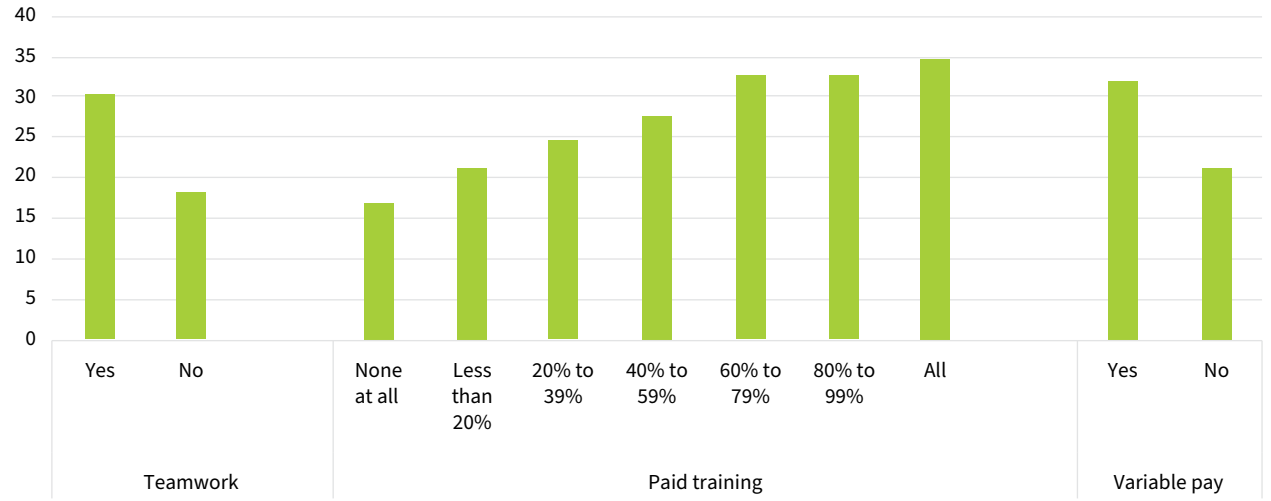
Figure 6: Use of data analytics to monitor employee performance by different work organisation modalities, EU27 and the UK (%)



Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

The survey also provides information on different facets of what are called 'high-performance work practices', which are characterised, for example, by high levels of training, performance-related pay and teamwork (Figure 7). Based on management responses, in general, workplaces that exhibit such features are more likely to use data analytics to monitor employee performance.

Figure 7: Use of data analytics to monitor employee performance by the proportion of workplaces with high-performance workplace characteristics, EU27 and the UK (%)

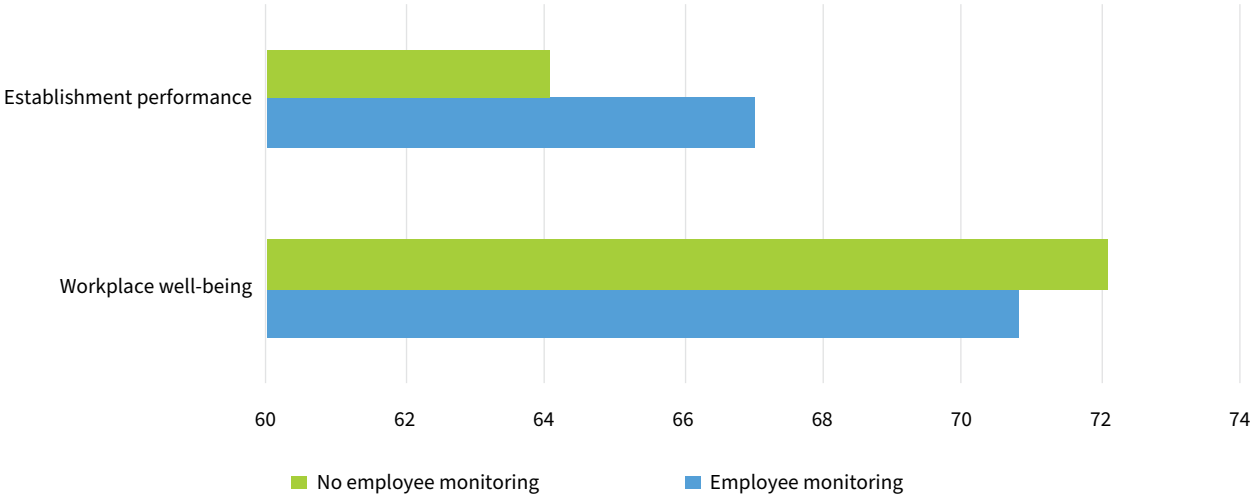


Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

One analysis of the ECS data used two composite indicators scaled 0–100 to monitor outcomes at establishment level in relation to workplace well-being, on the one hand, and establishment performance, on the other (Eurofound, 2020a). Four questions were used to indirectly measure workplace well-being: one captured the quality of the relationship between management and employees and the other three questions concerned challenges in terms of human resources (such as low motivation, absenteeism and staff retention). Establishment performance was measured in relation to the following four variables: the profitability of the establishments, the profit expectation, the change in production volume and the expected change in employment.

Using these two indicators, establishments in which data analytics were used to monitor employee performance were compared to those in which they were not. This indicated a lower score for workplace well-being and a higher score for establishment performance in establishments using these technologies (Figure 8). These differences are significant and remained significant when controls were introduced for establishment size, sector and country.

Figure 8: Use of data analytics to monitor employee performance and workplace outcomes, EU27 and the UK (%)



Source: *ECS 2019 management questionnaire (Eurofound, 2020a)*

Buffers of adverse effects of employee monitoring

In a laboratory study, Alge (2001) found that, by limiting internet monitoring to job-relevant activities and affording those who are monitored the opportunity to provide input into the process, the perceived invasion of privacy was reduced while the perceived procedural justice – that is, the perceived fairness of procedures used in the organisation – was enhanced. Alge (2001) argued that perceived fairness is an important determinant of employees' reactions to internet monitoring systems, and the way these systems are implemented influences employees' assessment of their fairness. Along similar lines, research conducted by Tabak and Smith (2005) found that the use of electronic performance monitoring was positively correlated with employee satisfaction and acceptance, provided that the monitoring was disclosed beforehand and employees had a voice. Fairness in the use of electronic monitoring systems was also studied by Alder et al (2006) in a longitudinal field experiment. The research found, however, that neither advance notice nor justification affected perceptions of monitoring fairness, but trust in the organisation did.

Qualitative research exploring employees' views on monitoring in British workplaces (Lockwood, 2018) suggests that employees accept monitoring when it is fully explained and communicated through a formal process and they are asked for their consent. While the majority of employees interviewed in this study expressed the view that monitoring within the work environment was acceptable, monitoring outside the workplace was not considered acceptable. In contrast, managerial representatives in the study viewed monitoring of their employees' use of the company's business systems as the employer's right and considered it reasonable as a means of ensuring that work was being performed to an appropriate standard.

Research also suggests that the extent of monitoring shapes the way monitoring is perceived by employees. When monitoring is perceived as excessive, it leads to absenteeism and higher employee turnover, lower morale, diminished trust in management and poorer employee–employer relations (Lockwood, 2018). The type of monitoring used may also influence how employees respond to it (Jeske and Kapasi, 2017). For example, research conducted by McNall and Roch (2007) found that video surveillance and 'eavesdropping' (recording of and listening to telephone conversations) tended to be perceived more negatively, in terms of interpersonal justice[16] and the invasion of personal privacy, than computer monitoring, which was defined in the study as keystroke recording, capturing only work-related computer activities.

16 The concept of interpersonal justice refers to the extent to which people feel they are treated with politeness, dignity and respect by an authority enacting a procedure (Colquitt et al, 2001).

In brief

- Research suggests that electronic employee monitoring influences employees' behaviour, potentially limits work autonomy and negatively affects employees' well-being and trust in management. The use of real-time and always-on monitoring technologies may also introduce game-like dynamics, which can place additional pressures on workers to meet performance targets.
- European Company Survey (ECS) data show that the use of data analytics to monitor employee performance correlates with the use of machines or computers. At the same time, establishments exhibiting features of high-performance work practices – for example, high levels of training, performance-related pay and teamwork – are more likely to use data analytics to monitor employee performance. The analysis also shows that establishments using data analytics to monitor employee performance have better outcomes in terms of establishment performance than establishments that make no use of data analytics to monitor employee performance. There is, however, a small and negative association between the use of data analytics for monitoring employee performance and workplace well-being.
- The implementation of intrusive and excessing monitoring in the workplace can have unintended consequences and can be counterproductive, not only by leading to a deterioration of aspects of job quality, but also by negatively affecting organisational performance. Research suggests that the type and extent of monitoring, as well as employee involvement, are important variables that can influence outcomes. All in all, there is a fine balance to be struck between the legitimate business interests of the employer and employees' right to privacy and expectations in this regard.

4 Concluding remarks

New digital technologies have entered the workplace, immeasurably expanding the possibilities of employee monitoring and surveillance. Monitoring technologies can be deployed to benign effect by responsible employers. However, because advanced digital technologies are increasingly versatile and lend themselves to different uses, there is concern that, once a technology is introduced into the workplace, it could be used for more intrusive means, sometimes even without the employee being totally aware of it.

Technological advances also challenge the very notion of acceptability for both employers and employees, making it possible to cross ethical boundaries. With constant exposure to smart and connected devices, there is a risk of passive acquiescence in the use of personal data both within and outside the workplace.

Digitally enabled employee monitoring may become more commonplace as remote working becomes more widely accepted by both employers and employees. There are increasing concerns – voiced in particular by trade unions – regarding the invasion of privacy as a result of the increased monitoring of remote workers. Intrusive digital monitoring can also generate tensions and undermine employment relations, including for those working in traditionally mobile occupations who are accustomed to more autonomy and discretion. Equally, existing concerns regarding employees' right to disconnect – which is already enshrined in national legislation in some Member States (Eurofound, 2020c) – will become more prominent if, as predicted, a higher proportion of paid work is done from home or from outside the employer's premises. While teleworkers may have to connect to be able to work, this should not imply assent to ongoing surveillance or monitoring outside work hours.

The boundaries of workers' privacy are challenged when monitoring extends to the tracking of non-work-related activities, especially in the case of technologies such as GPS location tracking, computer-monitoring software, wearables and remote sensors. Such invasive monitoring also raises concerns and questions in relation to the ability of the worker to give consent to or opt out of the collection of personal information. In addition, the notion of employee consent as specified in some national legislation is not a valid ground for processing personal data owing to the imbalance of power in the employment relationship. Employees may agree to monitoring and surveillance out of the fear of retaliation on the part of the employer and the potential loss of their job.

The EU General Data Protection Regulation – which has been implemented in national legislation in all countries – has modernised the data protection framework by enhancing the rights and protections of individuals in terms of their personal data, and this is applicable to the employment context. As surveillance technology continues to advance, it is important for European countries to stay alert, ensure that the existing rules are enforced and set boundaries to protect workers' fundamental rights.

Employers have a duty of care vis-à-vis their employees, and the transparency of their data collection practices is paramount, especially in the context of new digital technologies introduced into the workplace. Employees should be fully involved in the formulation of a clear data policy, with guidelines stating clearly the reasons for the collection and use of the data.

The available body of research on employee monitoring suggests that autonomy is reduced in situations where employee monitoring is intrusive and constant. The constraints on autonomy engendered by intrusive monitoring can erode employees' trust in their employer, which is at the core of the psychological contract between employer and employee. Monitoring systems have to be designed and implemented in a way that preserves workers' autonomy and must be in full compliance with data protection rules. Collective bargaining and social dialogue have an important role to play in both the design and the implementation of fair and transparent monitoring systems in the workplace.

Data-driven and evidence-based work management and human resources practices – powered by artificial intelligence (AI), the internet of things (IoT) and other digital technologies – may accentuate hierarchies and introduce new forms of – potentially oppressive – surveillance in the workplace. The use of algorithms, data and AI in human resources and recruitment also open up avenues for discrimination. The principles of transparency and responsibility should be applied by employers to avoid any misuse of AI-based work management and recruitment systems.

The debate around the use of digitally enabled employee monitoring is often framed by concerns about ethics, privacy and data protection. Pervasive and constant surveillance at work not only impinges on workers' right to privacy, but also interferes with the right to freedom of association and collective bargaining, and the right to mental and physical health, generating tensions in the workplace and creating a negative work environment. Both employees and employers lose out when employee monitoring and surveillance practices are intrusive and non-transparent. The many implications of employee monitoring and surveillance for job quality and work organisation warrant more attention in policy debate.

Bibliography

All Eurofound publications are available at www.eurofound.europa.eu

Alder, S. G., Ambrose, M. L. and Noel, T. W. (2006), 'The effect of formal advance notice and justification on internet monitoring fairness: Much about nothing?', *Journal of Leadership and Organisational Studies*, Vol. 13, No. 1, pp. 93–108.

Alge, B. J. (2001), 'Effects of computer surveillance on perceptions of privacy and procedural justice', *Journal of Applied Psychology*, Vol. 86, pp. 797–804.

AlgorithmWatch (2020), *People analytics must benefit the people. An ethical analysis of data-driven algorithmic systems in human resources management*, Berlin.

Aloisi, A. and Gramano, E. (2019), 'Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context', *Comparative Labour Law and Policy Journal*, Vol. 41, No 1, pp. 95–121.

AP (Autoriteit Persoonsgegevens) (2013), *Onderzoek naar het gebruik van (heimelijke) camera's door*

Media Markt-Saturn Holding Nederland B.V., The Hague

AP (2015), *Onderzoek naar video-opnames van vrachtwagenchauffeurs met de eventrecorder door transportbedrijf De Rooy Transport B.V.,* The Hague.

Azevedo, F. M. (2018), 'GPS – meio de vigilância à distância e a sua repercussão no direito à reserva da intimidade da vida privada do trabalhador', Revista Julgar Online, March.

Ball, K. (2010), 'Workplace surveillance: An overview', *Labour History*, Vol. 51, No. 1, pp. 87–106.

Billinghurst, M. and Starner, T. (1999), 'Wearable devices: New ways to manage information', *Computer*, Vol. 32, No. 1, pp. 57–64.

Bråten, M. (2016), *Digital kontroll og overvåking av arbeid: Omfang og praksis*, Fafo, Oslo.

Bråten, M. (2017), 'Bruk av digitale kontrollteknologier og ivaretakelse av personvern i arbeidsforhold', *Magma*, Vol. 6/2017, pp. 54–62.

Bråten, M. (2019), *Kontroll og overvåking i arbeidslivet*, Fafo, Oslo.

Bråten, M. and Tranvik, T. (2017), 'The visible employee – Technological governance and control of the mobile workforce', *Socio-Economic Studies*, Vol. 28, No. 3, pp. 319–337.

Brynjolfsson, E., Rock, D. and Syverson, C. (2017), *Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics*, Working Paper No. 24001, National Bureau of Economic Research, Cambridge, MA, USA.

BusinessEurope (Confederation of European Business) (2020a), 'Europe's digital masterplan: A push into the digital age', press release, 19 February.

BusinessEurope (2020b), 'The GDPR in review: A good start but improvement necessary', press release, 24 June.

Business Insider (2014), 'How this company knows you're going to quit your job before you do', 19 November.

Business Insider (2018), 'Fitbit's moving away from a simple step counter into health coaching as it faces competition from the Apple Watch', 22 September.

Business Insider (2020), 'Companies are using webcams to monitor employees working from home', 23 March.

Canteiro, P. (2017), 'As redes sociais e a des(proteção) da privacidade do trabalhador', conference paper, *O Direito do Trabalho e as Empresas: Novos desafios, Novas Soluções?*, Atas do IX Congresso Internacional de Ciências Jurídico-Empresariais, 10 October 2017, Escola Superior de Tecnologia e Gestão de Leiria, Portugal.

Casilli, A. A. (2019), *En attendant les robots: Enquête sur le travail du clic*, Seuil, Paris.

CGT (Confédération Générale du Travail) (2019), *Fin de non recevoir pour la reconnaissance faciale*, web page, accessed 30 September 2020.

Chory, R. M., Vela, L. E. and Avtgis, T. A. (2016), 'Organizational surveillance of computer-mediated workplace communication: Employee privacy concerns and responses', *Employee Responsibilities and Rights Journal*, Vol. 28, pp. 23–43.

CIPD (Chartered Institute of Personnel and Development) (2017), *Employee outlook: Employees' views on working life*, London.

CNIL (Commission Nationale de l'Informatique et des Libertés) (2018), *Rapport d'activité 2018*, La Documentation Française, Paris.

CNIL (2019), *Facial recognition: For a debate living up to the challenges*, web page, accessed 30 September 2020.

Colquitt, J., Conlon, D., Wesson, M., Porter, C. and Ng, K. (2001), 'Justice at the millennium: A meta-analytic review of the 25 years of organizational justice research', *Journal of Applied Psychology*, Vol. 86, pp. 425–445.

Croatian Graphical Union (undated), *Nadzor na radnom mjestu - Pazite – snimaju vas*, web page, accessed 25 September 2020.

DARES (Directorate of Research, Economic Studies and Statistics) (2019), *Comment ont évolué les expositions des salariés du secteur privé aux risques professionnels sur les vingt dernières années? Premiers résultats de l'enquête Sumer 2017*, DARES Analyses, No. 41, Paris.

Datatilsynet (2019), *Årsrapport for 2018: Tall og tendenser fra Datatilsynets virksomhet*, Oslo.

Deloitte (2018), 'Wearables are augmenting employees' abilities', *Deloitte Insights*, 25 July.

Deloitte (2019), *Undersøkelse om overvåking: Tyder på manglende retningslinjer i norske virksomheter – Elektronisk overvåkning i norske virksomheten*, web page, accessed 30 September 2020.

Digital Freedom Fund (2019), *Harnessing existing human rights jurisprudence to guide AI*, web page, accessed 30 September 2020.

ECtHR (European Court of Human Rights) (2007), 'Judgment in the case of Copland v the United Kingdom (Grand Chamber)', no. 62617/00, 3 April 2007, Strasbourg.

ECtHR (2017) 'Judgment in the case of Bărbulescu v Romania (Grand Chamber)', no. 61496/08, 5 September 2017, Strasbourg.

ECtHR (2018), 'Judgment in the case of Antovic and Mirkovic v Montenegro (Second Section)', no. 70838/13, 28 February 2018, Strasbourg.

ECtHR (2019), 'Judgment in the case of López Ribalda and Others v Spain (Grand Chamber)', nos. 1874/13 *and* 8567/13, 17 October 2019, Strasbourg.

EDPB (European Data Protection Board) (2020), *Guidelines 05/2020 on consent under Regulation 2016/679*, adopted on 4 May 2020.

ETUC (European Trade Union Confederation) (2016), *ETUC resolution on digitalisation: Towards fair digital work*, Brussels.

ETUC (2020), 'ETUC response to Commission strategies on digital and AI', press release, 19 February.

ETUC, BusinessEurope, CEEP and SMEUnited (2020), *European social partners framework agreement on digitalisation*, Brussels.

ETUI (European Trade Union Institute) (2020), *Labour in the age of AI: Why regulation is needed to protect workers*, Foresight Brief, Brussels.

Eurofound (2008), *New employee chamber brings workers together in single status*, web page, accessed 25 September 2020.

Eurofound (2018), *Automation, digitisation and platforms: Implications for work and employment*, Publications Office of the European Union, Luxembourg.

Eurofound (2020a), *European Company Survey 2019: Workplace practices unlocking employee potential*, Publications Office of the European Union, Luxembourg.

Eurofound (2020b), *Game-changing technologies: Transforming production and employment in Europe*, Publications Office of the European Union, Luxembourg.

Eurofound (2020c), *Regulations to address work–life balance in digital flexible working arrangements*, New forms of employment series, Publications Office of the European Union, Luxembourg.

Eurofound (2020d), *Telework and ICT-based mobile work: Flexible working in the digital age*, New forms of employment series, Publications Office of the European Union, Luxembourg.

European Commission (2018), *Biometrics technologies: A key enabler for future digital services*, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Brussels.

European Commission (2020a), *A European strategy for data*, COM(2020)66 final, Brussels.

European Commission (2020b), *Big data*, web page, available at https://ec.europa.eu/digital-single-market/en/big-data, accessed 30 September 2020.

European Commission (2020c), *On artificial intelligence – A European approach to excellence and trust*, COM(2020)65 final, Brussels.

European Parliament (2019), *Health and safety in the workplace of the future*, Directorate-General for Internal Policies of the Union, Brussels.

EuroWeekly (2020), 'Swedes get futuristic high tech implants in their hands to replace cash and credit cars, eliminating Coronavirus contact', 10 April.

Evz.ro (2008), 'Atenţie, angajaţi: şeful află orice mişcare!', 21 April.

Ezquerra, L. (2018), *Nuevas tecnologías en el control de los trabajadores y el derecho a la intimidad del trabajador*, web page, accessed 30 September 2020.

Financial Times (2018), 'How AI helps recruiters track jobseekers' emotions', 28 February.

Financial Times (2020), 'The danger of Alphabet's move into the risk business', 1 September.

FOA (Fag og Arbejde) (2018), *Hver sjette sosu bliver overvåget på jobbet*, web page, accessed 30 September 2020.

Forbes (2017), 'How to drive employee engagement with workplace gamification', 28 November.

Forbes (2018), 'The amazing ways how Unilever uses artificial intelligence to recruit and train thousands of employees', 14 December.

FRA (European Fundamental Rights Agency) and Council of Europe (2018), *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg.

Furnham, A. and Swami, V. (2015), 'An investigation of attitudes toward surveillance at work and its correlates', *Psychology*, Vol. 6, pp. 1668–1675.

Fyens Stiftstidende (2019), 'Når chefen kigger med', 24 June.

GPDP (Garante per la protezione dei dati personali) (2020), 'Audizione del Presidente del Garante per la protezione dei dati personali sull'affare assegnato atto n. 453 relativo al tema Ricadute occupazionali dell'epidemia da Covid-19, azioni idonee a fronteggiare le situazioni di crisi e necessità di garantire la sicurezza sanitaria nei luoghi di lavoro', Commission 11a (Public and private work, social security) of the Senate of the Republic of Italy, 13 May.

Garzia, C. (2013), *Workplace surveillance: Good watchdog or cynical control?,* unpublished master's thesis, University of London.

Gillet, I., Greenan, N. and Le Gall, R. (2016), *Les effets de la surveillance électronique: Une expérimentation dans un centre d'appels*, Collection Espaces Numériques, Cigref, Editions Lavoisier, Paris.

Gumzej, N. and Dragičević, D. (2019), 'Video surveillance in the workplace under the Croatian act on implementation of the general data protection regulation', *Zbornik Pravnog fakulteta u Zagrebu*, Vol. 69, No. 3, pp. 327–346.

Hanley, D. A. and Hubbard, S. (2020), *Eyes everywhere: Amazon's surveillance infrastructure and revitalizing worker power*, Open Markets Institute.

IAPP (International Association of Privacy Professionals) (2016), *How big will big data be under the GDPR?*, web page, accessed 30 September 2020.

Ienca, M. and Andorno, R. (2017), 'Towards new human rights in the age of neuroscience and neurotechnology', *Life Sciences, Society and Policy*, Vol. 13, No. 5.

ILO (International Labour Organization) (1997), *Protection of workers' personal data: An ILO code of practice*, Geneva.

ILO (undated), *The text of the Declaration and its follow-up*, web page, accessed 24 September 2020.

Independent (2017), 'Barclays installs sensors to see which bankers are at their desks', 19 August.

INSHT (Instituto Nacional de Seguridad e Higiene en el Trabajo) (2015), *Estrategia Española de Seguridad y Salud en el Trabajo 2015–2020*, Madrid.

Irish Independent (2013), 'Tesco staff forced to wear arm monitors that track work rate', 11 February.

Jeske, D. and Kapasi, I. (2017), 'Electronic performance monitoring: Lessons from the past and future challenges', conference paper, Annual Conference of the Italian Chapter of the Association of Information Systems (ItAIS), 5–7 October, Milan.

Kanngieser, A. (2013), 'Tracking and tracing: geographies of logistical governance and labouring bodies', *Environment and Planning D: Society and Space*, Vol. 31, pp. 594–610.

Keyriläinen, M. and Sutela, H. (2018), 'Suomalaisten palkansaajien kokemuksia työn digitalisaatiosta', *Työelämän tutkimus – Arbetslivsforskning*, Vol. 16, No. 4, pp. 275–288.

Lexology (2019), 'Employee surveillance in GDPR era', 4 December.

LO (Norwegian Confederation of Trade Unions) and NHO (Confederation of Norwegian Enterprise) (2019), *Basic agreement, 2018–2021, LO–NHO with supplementary agreements*, Oslo.

Lockwood, G. (2018), 'Workplace monitoring and surveillance: The British context', *Athens Journal of Law,* Vol. 4, No. 3, pp. 205–228.

McNall, L. A. and Roch, S. G. (2007), 'Effects of electronic monitoring types on perceptions of procedural justice, interpersonal justice, and privacy', *Journal of Applied Social Psychology*, Vol. 37, pp. 658–682.

McNall, L. A. and Stanton, J. M. (2011), 'Private eyes are watching you: Reactions to location sensing technologies', *Journal of Business and Psychology*, Vol. 26, pp. 299–309.

McParland, C. and Connolly, R. (2019), 'Employee monitoring in the digital era: Managing the impact of innovation', conference paper, ENTRENOVA – Enterprise Research Innovation Conference, 12–14 September, Rovinj, Croatia.

Mamia, T., Alvesalo-Kuusi, A., Kuokkanen, A. and Virtanen, S. (2011), *Työn elektroninen valvonta Suomessa*, Finnish Institute of Occupational Health, Helsinki.

Mateescu, A. and Nguyen, A. (2019), *Workplace monitoring and surveillance*, Data and Society Research Institute, New York.

Ministry of Economic Affairs and Employment in Finland (undated), *Act on Co-operation Within Undertakings is not just a law on terminating employment*, web page, available at https://tem.fi/en/negotiation-obligation, accessed 25 September 2020.

Moreira, T. (2016), 'The electronic control of the employer in Portugal', *Labour and Law Issues*, Vol. 2, No. 1.

NFC World (2018), 'Telecoms boss gets NFC access control chip implanted in hand', 16 October.

OECD (Organisation for Economic Co-operation and Development) (2019), *Recommendation of the Council on responsible innovation in neurotechnology*, Paris.

Oliver, H. (2002), 'Email and internet monitoring in the workplace: information privacy and contracting-out', *Industrial Law Journal*, Vol. 31, pp. 321–352.

Organise (2018), *Amazon: What's it like where you work? Findings from the Amazon Warehouse Employee survey*, London.

Owczarek, D. and Chełstowska, A. (2016), *Amazon po Polsku. Warunki pracy i stosunki z pracownikami*, Instytut Spraw Publicznych and Friedrich-Ebert-Stiftung – Representation in Poland, Warszawa.

Oxfordshire County Council (2018), *Recycling staff to get body worn cameras*, web page, accessed 30 September 2020.

Pritchard, G., Briggs, P., Vines, J. and Oliver, P. (2015), 'How to drive a London bus: measuring performance in a mobile and remote workplace', conference paper, 33rd Annual ACM Conference on Human Factors in Computing Systems. Seoul, 18–23 April 2015.

Prospect (2020), *Future of work: Employers' collection and use of worker data*, Prospect briefing, London.

PwC (Pricewaterhouse Coopers) (2016), *Wearable technology in the workplace: are employees ready?*, web page, accessed 30 September 2020.

Ravid, D. M., Tomczak, D. L., White, J. C. and Behrend, T. S. (2019), 'EPM 20/20: A review, framework, and research agenda for electronic performance monitoring', *Journal of Management*, Vol. 46, No. 1, pp. 100–126.

Regjeringen (2018), *Personvernkommisjon – innspill til mandat*, web page, accessed 25 September 2020.

Reuters (2018), 'Amazon scraps secret AI recruiting tool that showed bias against women', 10 October.

Rimmelzwaan, J. (2017), 'Use of a wearable device to promote healthy behaviors among employees of a small-to-medium enterprise in the Netherlands', in Adams, S., Purtova, N. and Leenes, R. (eds.), *Under observation: The interplay between ehealth and surveillance*, Springer, Berlin, pp. 59–72.

Rosengren, C. and Ottosson, M. (2016), 'Employee monitoring in a digital context', in Daniels, J., Gregory, K. and McMillan Cottom, T. (eds.), *Digital sociologies*, Policy Press, Bristol, pp. 181–194.

Rousseau, D. M. (1995), *Psychological contracts in organizations: Understanding written and unwritten agreements*, Sage, Thousand Oaks, CA, USA.

Rožman, K. (2018), 'Videonadzor u radnim odnosima: Dvojbe i pitanja' (Video surveillance in employment: Doubts and questions), *Radno pravo*, Vol. 15, No. 7–8, pp. 11–24.

SACO (Swedish Confederation of Professional Associations) (2016), *Integritet och Kontroll i Arbetslivet*, Stockholm.

SAK (Central Organisation of Finnish Trade Unions) (2018), *SAK:n työolobarometri 2018*, web page, accessed 30 September 2020.

Schubert, C. and Hütt, M. T. (2019), 'Economy-on-demand and the fairness of algorithms', *European Labour Law Journal*, Vol. 10, No. 1.

SMEUnited (Association of Crafts and SMEs in Europe) (2019), *GDPR application discussed: Mandatory monitoring body not fit for SMEs*, web page, accessed 30 September 2020.

Sostero, M., Milasi, S., Hurley, J., Fernandez-Macias, E. and Bisello, M. (2020), *Teleworkability and the COVID-19 crisis: A new digital divide?*, JRC Working Papers Series on Labour, Education and Technology 2020/05, European Commission, Seville.

Statistics Finland (2020), *Quality of work life*, web page, available at https://www.stat.fi/meta/til/tyoolot_en.html, accessed 15 October 2020.

Statistical Service of Cyprus (2019), *Labour Force Survey ad-hoc module 2019 – Work organization and working time arrangements*, web page, available at https://www.mof.gov.cy/mof/cystat/statistics.nsf/labour_31main_keyfarchive_en/labour_31main_keyfarchive_en?OpenForm&yr=2019C2F83D54DCEF1189555DA9B7BEFE-3B9E&n=2019, accessed 30 September 2020.

Stoney, A. G. and Tompkins, P. K. (1997), 'Electronic performance monitoring: An organizational justice and concretive control perspective', *Management Communication Quarterly*, Vol. 10, No. 3, pp. 259–289.

Sutela, H., Pärnänen, A. and Keyriläinen, M. (2019), *Digiajan Työelämä – Työolotutkimuksen tulokisa 1977–2018*, Statistics Finland, Helsinki.

Tabak, F. and Smith, W. (2005), 'Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development', *Employee Responsibilities and Rights Journal*, Vol. 17, No. 3, pp. 173–189.

The Guardian (2016), 'Daily Telegraph to withdraw devices monitoring time at desk after criticism', 11 January.

The Guardian (2018a), 'Alarm over talks to implant UK employees with microchips', 11 November.

The Guardian (2018b), 'Amazon patents wristband that tracks warehouse workers' movements', 1 February.

The Guardian (2020), 'Barclays using "Big Brother" tactics to spy on staff, says TUC', 20 February.

The New York Times (2018), 'If workers slack off, the wristband will know (and Amazon has a patent for it)', 1 February.

The Telegraph (2018), 'Privacy concerns over Amazon plans for augmented reality goggles that track warehouse workers', 3 August.

The Verge (2020), 'Amazon deploys AI "distance assistants" to notify warehouse workers if they get too close', 16 June.

The Wall Street Journal (2015), 'The algorithm that tells the boss who might quit', 13 March.

The Washington Post (2020), 'Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home', 30 April.

Thon, B. E. (2015), Op-ed in *Fri Fagbevegelse*, 20 January.

Torpey, J. (2007), 'Through thick and thin: Surveillance after 9/11', *Contemporary Sociology*, Vol. 36, No. 2, pp. 116–119.

TUC (Trades Union Congress) (2018), *I'll be watching you: A report on workplace monitoring,* London.

UGT (Unión General de Trabajadores) (2019a), *Protocolo de actuacion para la negociacion colectiva. Protección de datos de caracter personal y garantias de los derechos digitales*, Madrid.

UGT (2019b), *Incidencia de las nuevas tecnologías de la información y de la comunicación en la seguridad y salud de los trabajadores*, Madrid.

UNI Europa (2020), 'Commission's AI policy: Some progress but still too little to protect workers', press release, 20 February.

UNI Global Union (2020), 'UNI Global Union launches new push for collective bargaining around algorithmic management tools', press release, 1 September.

Wachter, S. and Mittelstadt, B. D. (2019), 'A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI', *Columbia Business Law Review*, No. 1.

Wiadomosci Handlowe (2019), 'Alfred Bujara, NSZZ Solidarność: Cyfrowa inwigilacja pracowników handlu coraz większym problemem', 21 October.

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

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

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres.
You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union.
You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: http://europa.eu/contact

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications

You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

EF/20/008

New digital technologies have expanded the possibilities of employee monitoring and surveillance, both in and outside the workplace. In the context of the increasing digitalisation of work, there are many issues related to employee monitoring that warrant the attention of policymakers. As well as the often-cited privacy and ethical concerns, there are also important implications for worker–employer relations, as digitally enabled monitoring and surveillance inevitably shift power dynamics in the workplace. Based on input from the Network of Eurofound Correspondents, this report explores the regulatory approaches to workplace monitoring in Europe, and the many challenges arising from the use of new digital technologies. Drawing from empirical and qualitative research, the report also provides some insight into the extent of employee monitoring in Europe and the implications for job quality and work organisation.

The European Foundation for the Improvement of Living and Working Conditions (Eurofound) is a tripartite European Union Agency established in 1975. Its role is to provide knowledge in the area of social, employment and work-related policies according to Regulation (EU) 2019/127.

Publications Office
of the European Union