9

Telework and Digital Surveillance

Legal Challenges on the Interface of Labour and Data Protection Law

Elias Felten

9.1 INTRODUCTION

The rapid acceleration of digitalisation in industries and services over the past decade has had a direct impact on the organisation of labour. While telework is now primarily associated with the COVID-19 pandemic, it is fundamentally a result of the growing significance of information technology in both our professional and personal lives. Today, even manual labour is frequently supported by digital technologies, making data processing an integral part of virtually every employment relationship. This applies not only to employees working on-site but particularly to those working remotely. In fact, the rise of remote work as a widespread phenomenon is largely due to the use of modern information technologies.

However, the organisational changes in work resulting from digitalisation challenge the functionality and effectiveness of labour law. Data protection is becoming increasingly important in the labour context, and in many instances, labour protection and data protection can no longer be considered separately. Despite this, the law has not adequately evolved to reflect these changes.

This chapter will therefore at first analyse the existing shortcomings and gaps in the law also from a human rights perspective, using the issue of digital surveillance in telework as an example. In its second part, it aims to explore potential legal mechanisms to establish or even enhance the interaction between labour and data protection law.

9.2 TELEWORK AND CONTROL

Telework is nowadays the key for employees by which they can perform tasks remotely, outside of the employer's premises, in most cases (in the aftermath of the COVID-19-pandemic) at home. One potential benefit of combining telework with remote work is that it can help improve the balance between work and family

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

responsibilities. Employees who can work from home are able to respond more flexibly to family needs, such as caring for sick children. The elimination of commuting, furthermore, creates additional time that can be used for caregiving duties within the family. This view is shared by the European legislator, as reflected in the Work-Life Balance Directive 2019/1158/EU, which promotes flexible working arrangements, explicitly including remote work[1].

Remote work is, of course, only made possible in most cases by modern communication technologies. That is why remote work and telework usually go hand in hand. This is already expressed in the legal definition of telework, as defined by the framework agreement between European social partners[2]. The agreement defines telework as a 'form of organising and/or performing work, using information technology, in the context of an employment contract/relationship, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis'. Analysing this definition, the notion of 'telework' is characterised by a crucial criterion which distinguishes this so called 'flexible working agreement' from traditional organised work: It is not merely the use of information technologies to perform tasks; after all, many employees working on their employer's premises use such technologies as well. The defining feature is that employees provide their services 'away from the employer's premises'. Even though employees working off-site, such as at a client's office or home, have long existed, they represented a small minority. Since the COVID-19-pandemic, however, the number of employees working at home has increased significantly.

9.2.1 *Monitoring Measures: An Integral Part of Telework*

The organisational impact of telework, namely, the separation of employer and employee by location, has gained greater importance and introduced one specific new qualitative challenge: employers are no longer able to personally verify whether their employees are fulfilling their contractual obligations. This marks a shift in the approach to human resource management. Employers are increasingly aiming to encourage employees to work more independently and to focus on results, with the goal of boosting productivity. Management by objectives is perhaps the most well-known expression for this management style. This increase in independence, however, is naturally accompanied by a loss of control on the employer's side. That is the reason why in many cases technical control measures, sometimes disguised as mere performance evaluation tools, come into play when it comes to telework[3].

Some might argue that the situation on the employer's premises is not significantly different, given the large number of employees. No employer can personally

[1] Cf Article 3 (1) lit f Directive 2019/1158/EU.
[2] https://eur-lex.europa.eu/EN/legal-content/summary/teleworking.html.
[3] Vitak and Zimmer (2023, 1).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

supervise every individual. This is true to a certain extent. However, on-site, the limitations of direct supervision are often compensated for by 'social pressure' exerted by management and colleagues[4]. If a division manager fails to report an employee's unexcused absence, colleagues are likely to do so. This is the key distinction between working remotely, such as from home, and working on-site. At home neither the social pressure exerted by colleagues nor any other compensatory control mechanisms, such as clients noticing an employee's tardiness to a meeting, apply to close this gap. As a result, the employer's understandable concerns that an employee may focus on personal matters rather than work-related tasks serve to justify, in practice, the implementation of more stringent monitoring measures. These measures are designed to ensure that employees perform their duties in both the required quantity and quality.

However, the scope of monitoring measures extends even further: to a certain degree, they replace the employer's direct authority. While the employer may not be physically present in the employee's home, the sense of their presence can actually be stronger due to pervasive surveillance measures enabled by AI-driven collaboration platforms commonly used in telework. This creates a significant paradox: although teleworkers appear to enjoy greater autonomy by working remotely free from the employer's immediate physical oversight, they are simultaneously subjected to greater dependency[5]. The employer's authority becomes more dispersed yet concentrated through digital control mechanisms.

This trend is reinforced by the fact that monitoring tools can be easily, inexpensively and highly effectively implemented, as they are now an integral part of modern, especially AI-based, communication and collaboration technology[6]. In fact, the provision of digital workplace monitoring tools has evolved into a distinct business sector, with a growing number of software vendors offering such solutions in recent years[7].

9.2.2 *Monitoring Measures: The Impact of Data Protection Law*

The justification for implementing monitoring software, however, is not limited to the employer's legitimate interest of ensuring the employee's compliance with the labour contract and maintaining managerial authority beyond the workplace. Data protection law can also support this rationale, because telework is inconceivable without data processing. However, even when an employee works remotely and processes data from home, the employer still determines the purpose and means of data processing. This is because the employer's role as a 'controller' in the sense of

[4] Goricnik (2021, 150).
[5] Jervis (2018, 449).
[6] Jervis (2018, 448); Nurse et al. (2021, 5).
[7] Aloisi and De Stefano (2022, 298); Auer-Mayer (2020/88).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

Article 4 (7) GDPR does not depend on the location where the employee is working.

As the data controller, the employer is responsible under Article 24 (1) GDPR for implementing appropriate technical and organisational measures to ensure, and demonstrate, that data processing complies with the GDPR. In other words, the employer is required to establish a data protection policy. In accordance with Article 32 GDPR, this policy must include specific measures to address the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data that is transmitted, stored or otherwise processed. It is the responsibility of the controller, that is, the employer, to decide which measures are appropriate to achieve these objectives. However, when determining these specific measures, the 'nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons' must be considered, as explicitly outlined in the GDPR. In summary, the greater the risk of a potential data breach, the stronger the need for effective measures to ensure data protection and security.

Given the strict standards of European data protection law, there is no doubt that remote telework conducted from an employee's home poses a significant risk to the data protection rights of individuals. The employer is typically unable to ensure that other individuals, particularly family members, do not have access to sensitive data, nor can the employer guarantee that this data is stored securely[8]. The mere fact that family members share the same living space, or even the same room, as the employee must already be considered a risk. Additionally, the home infrastructure used to perform work-related tasks, such as internet access, falls outside the employer's control. This, in turn, may justify the implementation of extensive digital monitoring of teleworkers[9].

9.3 THE EMPLOYER'S RIGHT TO CONTROL: FOUNDATIONS AND BOUNDARIES

Considering the relationship between telework and monitoring, one must acknowledge that control is, of course, an integral part of any employment relationship. Even if it is not explicitly outlined in the employment contract, the employer's right to exercise control is implicitly agreed upon by both parties. It is, in fact, a reflection, and more importantly, a fundamental aspect, of the personal dependency that defines the employee's legal status under labour law. Since employees agree to provide services of a certain quantity and quality under the employer's direction, the employer has the right to monitor and verify whether the employee is fulfilling their contractual obligations. However, the employer's right to control is inherently linked

[8] WP29 (2017, 16).
[9] Ibid.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

to the employee as a person. This is a logical consequence of the nature of an employment contract, where the services provided cannot be separated from the individual providing them. As a result, control of the services inherently involves control of the individual performing those services.

9.3.1 *The Role of Fundamental Rights*

Nevertheless, the mutual agreement that the employer has a right to control does not imply that the employee has consented by these means to waive their personal rights. This statement is of central importance because individual personal rights are recognised and protected as human rights. The European Court of Human Rights recently made clear, that the right to respect for everyone's private life according to Article 8 includes also the legal obligation to take care of the employees' personal rights and their legitimate interests at the workplace[10]. That imposes the positive obligation to safeguard respect for private life in the relations between individuals, and therefore also between the labour parties, by setting up a legislative framework taking into consideration the various interests to be protected in a particular context[11]. That applies especially to monitoring measures set up by employers at the workplace, as the European Court of Human Rights pointed out: the right to respect for private life contains the obligation to ensure that the introduction of measures to monitor employees, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse[12]. One of these safeguards, according to the European Court of Human Rights, is the employer's obligation to provide legitimate reasons to justify monitoring employees. More invasive methods, therefore, require weightier justification[13].

The enshrinement of the right to respect for private life as a human and thus as a fundamental right would generally lead one to expect that it imposes effective limits on employers using technical measures to control employees, particularly at home. Although the human rights impact has been explicitly recognised by the European Court of Human Rights, the Court has also clarified that the scope and extent of such control measures depend on the employer's legitimate interest in monitoring their employees. In effect, this means that individual personal rights are not absolute but are contingent on the competing interests of the employer. What is noteworthy in this context is that these interests do not necessarily need to be backed by fundamental rights; rather, purely economic interests seem sufficient to justify intrusions into the right to respect of private life.

[10] Cf ECHR Barbulescu vs Romania Rc 70 ff.
[11] Cf ECHR Barbulescu vs Romania Rc 115.
[12] Cf ECHR Barbulescu vs Romania Rc 120.
[13] Cf ECHR Barbulescu vs Romania Rc 120.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

This is indicated by the case law of the European Court of Human Rights who concluded in a landmark case that GPS tracking of vehicles to monitor the distances driven by employees during work activities is consistent with Article 8 ECHR, provided the employer uses it to verify the accuracy of recorded daily, weekly and monthly activities, visits made, absences and business travel expenses. The Court recognised that by evaluating geolocation data related to distances travelled, the employer is pursuing the legitimate aim of monitoring the company's expenses which justifies GPS tracking of employees[14]. Or in other words: mere economic interests are sufficient justification for allowing significant interference with employees' personal rights.

This approach which makes the extent, duration and intensity of control measures contingent upon the employer's economic interests is on closer look highly problematic as data protection comes into play.

9.3.2 *The Role of Data Protection Law*

The conclusion that the employer can rely on legitimate interests in relation to employees working remotely is crucial for the introduction of digital monitoring measures, particularly from a data protection law perspective. Since digital surveillance of teleworkers inherently involves data processing, the requirements of data protection law, harmonised across the European Union through the regulatory instrument of a regulation, must also be fulfilled. According to the GDPR, any processing of personal data must be 'lawful' under Article 6 and, depending on the sensitivity of the data involved, under Article 9 as well. This could again serve as an effective limitation on invasive control measures by the employer, especially since the possibility of individual consent to monitoring measures is mostly not available at the time of entering into the employment contract. Article 7 GDPR requires 'freely given consent' to data processing. However, the element of voluntariness is notoriously absent in the employment relationship due to the structural imbalance between employee and employer and the resulting dependency[15].

Nonetheless, the GDPR provides other grounds under which data can be lawfully processed. In this context, Article 6 (1) lit f is particularly relevant, as it permits data processing if the processor again can demonstrate a legitimate interest. Although Article 6 (1) lit f GDPR does allow for the consideration of the employee's interests as well, especially when shaped by a fundamental right like the right to respect for private life, it is also true that these rights and freedoms must 'override' the interests of the data controller to prevent the processing of personal data. It is not sufficient if the employee's interests or fundamental rights are merely impacted; they must outweigh the controller's legitimate interests to limit data processing.

[14] Cf ECHR Florindo de Almeida Vasconcelos Gramaxo vs Portugal – 26968/16.
[15] Kotschy (2020, 330); Van Ecke and Simkus (2020, 1234).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

The possible consequences of this highly problematic legal approach to legitimate data processing by an assessment of interests shall be illustrated by the following example: Taking screenshots hourly with the purpose to check whether teleworkers are sitting and working at their desk is obviously striking the employee's personal rights. But at the same time, one could raise the question by which other means the employer shall control whether a teleworker is in fact fulfilling his or her duties to perform services in person at home? Would it not be lawful as well, if the employer enters the employees' offices at the employer's premise every hour to check whether they are present? Are the interests of the teleworkers in respecting their private lives indeed 'overriding' the employer's legitimate interests to check compliance with the labour contract in this case?

The GDPR does not give a concrete answer to these questions. That is the point where Article 8 ECHR might come into play. The enshrinement of the right to respect for private life as a human right would again lead one to expect that it imposes effective limits on employers processing personal employees' data considering that Article 6 (1) lit f GDPR is explicitly referring to the 'interests' and 'fundamental rights or freedoms' of the data subject. However, Article 8 ECHR does not seem to be the appropriate lever to strengthen employees' interests within this weighting, at least according to the interpretation of the European Court of Human Rights who stated that the employer's reliance on merely economic interests shall already be sufficient to justify close-knit geo-tracking of the employees' activities[16]. It is not to be expected that a stricter standard will be applied in data protection law. This is particularly true in light of the common legal doctrine on Article 6 (1) lit f GDPR which accepts every 'visible' interest not necessarily explicitly recognised by law as a legitimate interest of the controller, respectively, the employer[17].

Therefore, the importance of the GDPR setting up additional general principles for the processing of data must not be underestimated in practice, because they give at least certain guidelines for the concrete design of monitoring measures: Article 5 (1) lit a safeguards that the employee must be informed in advanced about the implementation of measures monitoring his or her activities. Furthermore, the obligation to delete data, which are no longer serving a legitimate purpose, can be extracted from Article 5 (1) lit e. However, once again, the general principles do not address the question to what extent the interests of the data subject must be considered for data processing to be considered lawful. And this once more is a loophole because it led the European Court of Human Rights to come to the conclusion that close-meshed geo-tracking serving the legitimate aim to monitor the company's expenditures is lawful as long as it was notified to the employee in advance and as long as the collected data gets deleted after checking the reported and registered activities[18]. Applied to the initial example of

[16] ECHR Florindo de Almeida Vasconcelos Gramaxo vs Portugal – 26968/16.
[17] Kotschy 2020, 337.
[18] ECHR Florindo de Almeida Vasconcelos Gramaxo vs Portugal – 26968/16.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

monitoring teleworkers through screenshots, this ruling leads to the following result: screenshots taken automatically every hour might be lawful in the light of the jurisdiction of the European Court of Human Rights as long as the employee has been informed in advance and as long as the screenshots get deleted after having checked that the employee is in fact present in his or her home office, which must be considered a legitimate employer's interest comparable to the interest of monitoring the company's expenses.

9.4 A LABOUR LAW APPROACH

This mechanism of Article 8 ECHR as well as of the GDPR allowing to weigh up every possible employer's interest – even merely economic interests – with employee's fundamental rights without setting standards for a proper balance is apparently a fundamental loophole of our existing set of laws which will probably cause even more problems in the near future. It seems evident that modern information technologies, particularly AI-driven systems, will increasingly permeate the organisation and execution of economic activities. These technologies will become even more crucial as means of production and operational resources for employers than they are today. Soon there will be no alternative, less intrusive measures that employers could use[19]. Consequently, the employer's interest in utilising them will also grow[20]. This is a reality that judges cannot ignore when balancing the conflicting interests of employers and employees. Therefore, it is very likely that the 'collateral damage' caused by these technologies, which enable comprehensive surveillance, will be accepted due to the lack of viable alternatives. In summary, the growing digitalisation will shift the balance of interests in favour of employers, which, under current regulations, will likely render even highly intrusive surveillance measures lawful[21].

However, this scenario of new technologies having unforeseeable and at the same time inevitable impacts on the personal rights of employees is not totally new. Only the dimension is probably unprecedented[22]. In fact, on the level of national labour law specific mechanisms were already designed in the past to safeguard that the personal rights of employees are respected properly and not overridden by the economic interests of the employer[23]. A central role in this context is played by collective representation of interests. From the outset, its function has been to balance the structural inequality between employees and employers. And, indeed, it has been shown that this approach can ensure fair working conditions for employees. This has ultimately led to the right to collective bargaining finally being

[19] Cf with regard to the 'least intrusive means test' Molè and Mangan (2023, 699).
[20] Cf also Van Ecke and Simkus (2020, 1236).
[21] Molè and Mangan (2023, 700).
[22] Aloisi and De Stefano (2022, 300).
[23] Aloisi and Gramano (2019, 108 f.)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

constitutionally protected by both the ECHR (Article 11) and the EU Charter of Fundamental Rights (Article 28).

In Austria[24] as well as in Germany[25] for instance, an employer's right to exercise control is contingent upon a collective agreement between the employer and the works council, the democratically elected and mandatory representative of all employees at the workplace. The involvement of the works council, along with the ability to apply collective pressure, aims to ensure that the personal rights of individual employees are adequately protected and that the specific control measures implemented are not overly intrusive[26]. In this way, collective labour law seeks to limit the employer's control to a legitimate purpose, ensuring it does not exceed what is necessary to achieve that aim. In other words, employees' participation shall prevent that personal dependency results in a system of total personal surveillance.

In practice, employers will need to offer specific commitments or guarantees to safeguard personal rights in order to reach an agreement with the works council. Without such an agreement, the employer is not permitted to introduce or implement monitoring measures. The obligation to engage in collective bargaining and reach an agreement is in fact a powerful tool to ensure that employees' interests are properly considered. To prevent the misuse of this bargaining power, German law provides employers with the option to apply for conciliation if an agreement with the works council cannot be reached[27]. Austrian labour law does not provide this possibility but requires the employer to reach an agreement, at least with regard to control measures which 'touch human dignity'[28]. So, for example, the introduction of new AI-based information technologies, enabling the employer to monitor the performance and activities of teleworkers in a very granular way, requires the involvement of the works council and therefore a consideration of the employees' interests under Austrian as well as under German law. The idea behind this legislation is that collective negotiations about the introduction and implementation of monitoring measures serve as a very effective legal instrument to safeguard the respect for employees' personal rights.

9.5 LABOUR LAW AND DATA PROTECTION LAW: FRIENDS OR FOES?

A comparable structural imbalance and thus the need to balance interests can be observed in relation to the processing of personal data for control purposes. On the one hand, employees are often unaware of or do not fully understand the monitoring capabilities associated with the use of digital information and communication technologies. On the other hand, there is a risk that employees may accept intrusive

[24] Cf Sect 96 para 1 no 3 and Sect 96a para 1 no 1 Arbeitsverfassungsgesetz (ArbVG).
[25] Cf Sect 87 para 1 no 6 Betriebsverfassungsgesetz (BetrVG).
[26] Krause (2020, 361).
[27] Sect 87 para 2 Betriebsverfassungsrecht (BetrVG).
[28] Sect 96 para 1 no 3 Arbeitsverfassungsgesetz (ArbVG).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

monitoring simply to secure the opportunity to work remotely. In this context, protecting individual privacy rights through collective representation in negotiations with the employer could be a viable approach.

However, implementing this mechanism, which ties an employer's authorisation to collect and process employees' personal data to the existence of a collective agreement, means that standards for protecting employees' individual interests may vary from company to company, depending on the specific agreement in place. The ability to develop tailored solutions through this process is undoubtedly a benefit. From a data protection law perspective, however, one might question whether the GDPR aligns with the Austrian and German approach, as the GDPR aims to establish a uniform and binding standard for the legality of data processing across all Member States. That is why the European legislator chose the legal instrument of a regulation whose introduction was justified by the need to ensure the proper functioning of the internal market[29]. Or to put it in the words of the CJEU: the regulation seeks to ensure the harmonisation of national legislation on the protection of personal data which is, in principle, complete[30]. As a consequence, according to the Court, Article 6 GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful[31]. The consent of employees' representatives through a collective agreement is not explicitly mentioned in this list, which is unsurprising given that the approach of data protection law is individualistic rather than collective.

9.5.1 *Data Protection through Collective Agreements*

However, the GDPR includes an important exception that allows Member States to introduce 'more specific rules', which can lead to deviations from the general standards established by the GDPR. According to Article 88 (1) 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 other words, Member States may introduce specific employment data protection provisions which do not necessarily have to follow one single common European standard. These 'more specific rules' can be based on 'laws' as well as 'collective agreements' according to the explicit wording of the GDPR. Article 88 (1) GDPR thus provides an opportunity for employee participation in finding a fair balance between the employer's and employees' interests regarding the processing of personal data.

[29] Cf Rec 13 of the GDPR 2016/67/EU.

[30] CJEU C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium, Rc 51.

[31] CJEU C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium, Rc 70.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

Thus, Article 88 (1) GDPR appears to be a suitable legal basis for integrating the labour law approach of protecting individual interests through collective means with the general principles of data protection law, especially concerning the lawfulness of monitoring measures. Article 88 (2) GDPR points out that those 'more specific rules' shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests, and fundamental rights, with particular regard to (among others) monitoring systems at the workplace. At first glance, Article 88 GDPR appears to facilitate a connection between data protection law and labour law mechanisms, such as those in Austrian and German law, which require employers to negotiate the introduction and implementation of monitoring measures with the works council[32].

A closer examination of the so-called 'opening clause' in Article 88 GDPR, however, may raise concerns about the interplay between labour and data protection law. Specifically, a range of complex legal questions emerges: Are only trade unions permitted to negotiate such 'more specific rules', or can works councils at the shop level, as foreseen in Austrian and German law, also engage in this process? The term 'collective agreement' in Article 88 (1) GDPR is not sufficiently clear in this point. Additionally, a works council in contrast to a trade union cannot invoke the right to collective bargaining guaranteed by Article 11 ECHR and Article 28 EU Charter of Fundamental Rights in this context, because their role is based on a legal obligation rather than the free will to participate. Moreover, the purpose of the GDPR to establish a common and coherent standard for data processing could support a restrictive interpretation as well. However, there is a strong argument that shop agreements are also included: Recital 155 of the GDPR refers explicitly to 'works agreements' explaining the consideration behind Article 88.

Another important question is whether the negotiating parties have complete freedom in shaping these specific measures to safeguard data subjects' human dignity in the context of monitoring systems, or if it is up to the legislator to define these measures? The CJEU recently stated that the Member States' discretion in adopting rules under Article 88 (1) GDPR is constrained by paragraph 2[33]. Hence, in order to be classified as a 'more specific rule' within the meaning of Article 88 (1) GDPR, the measures designed to protect employees' interests must meet the conditions outlined in paragraph 2 of that Article[34]. According to this provision, those more specific rules shall include 'suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing [. . .] and monitoring systems at

[32] Goricnik (2023, Tz 41).
[33] CJEU C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium, Rc 72.
[34] CJEU C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium, Rc 74.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

the work place'[35]. It may be questioned whether these requirements are met if the Austrian or German legislator only mandates employee participation in introducing monitoring measures without specifying parameters for the social partners on how to safeguard employees' human dignity and fundamental rights. Or, in other words, is it in line with Article 88 (2) if the legislator leaves it entirely up to the social partners to define the appropriate measures?[36] If this is not the case, would that not again infringe upon the autonomy of social partners and the right to collective bargaining protected by Article 11 ECHR and Article 28 EU Charter of Fundamental Rights? These questions clearly indicate that Articles 88 (1) and 88 (2) GDPR do not adequately account for the specific mechanisms and functioning of collective labour law. However, an interpretation that does not adequately recognise the bargaining autonomy of the social partners risks undermining the potential of the opening clause to serve as an effective interface between labour law and data protection law.

9.5.2 *Balancing of Interest through Collective Agreements*

Against this background, it is particularly important that there is another strong legal rationale for collective bargaining as a key instrument to protect employees' personal interests when they are subject to the processing of their personal data. According to Article 6 (1) lit f GDPR processing of data is lawful if the processing 'is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data'. To put it simply, the lawfulness of data processing depends on the balancing of interests. How this balancing of interests is to be carried out is, of course, left open by the European legislator. This is a big advantage, because it allows for the incorporation or application of labour law standards in this assessment. Referring again to Austrian legislation, it can be argued that within a system of collective negotiations, which does not provide for compulsory arbitration, the balance of interests required by Article 6 (1) lit f GDPR is achieved by the mere fact that the employer and employees' representatives reach a mutual agreement on the conditions and extent of personal data processing in the context of monitoring measures, provided that this agreement contains specific provisions to safeguard employees' personal rights as outlined in Article 88 (2). In other words, the fact that social partners have reached an agreement confirms in the sense of Article 6 (1) lit f GDPR that employees' fundamental rights and interests are considered properly and do not override the employer's interests in processing data[37]. This interpretation of Article 6 (1) lit f

[35] Cf also Van Ecke and Simkus (2020, 1234).
[36] Goricnik (2023, Tz 39).
[37] Felten and Preiss (2020, Tz 11).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

GDPR would ultimately lead to a coherent application of labour law and data protection law and would give space to collective bargaining also in the context of data processing and the protection of individual privacy rights.

9.6 CONCLUSION

The legal challenges linked to telework clearly highlight that one-dimensional solutions will in the future no longer be sufficient to guarantee adequate protection and appropriate working conditions for employees. This is particularly true when it comes to setting limits on extensive monitoring of teleworkers. The current labour law framework is increasingly proving inadequate on its own. Even the recognition of employees' rights as fundamental rights has had little effect on changing this. Due to the use of modern information and communication technologies, which inevitably involve the processing of employee data, data protection law must also be considered. While labour law and data protection law share structural similarities – both address a structural imbalance that must be mitigated through legal means – the tools and mechanisms used to achieve this goal differ significantly. In particular, the collective approach of labour law is alien to data protection law. However, as the example of teleworking shows, there are points of connection in existing law that make it possible to integrate the collective approach of labour law into data protection law, thereby closing existing protection gaps. This, however, currently requires significant interpretative effort, which entails a high degree of legal uncertainty for all parties involved, both employers and employees. It should, therefore, be the task of the European legislator to anchor data protection law more firmly to collective bargaining, as enshrined in the EU Charter of Fundamental Rights.

REFERENCES

Aloisi, Antonio and De Stefano, Valerio, Essential jobs, remote work and digital surveillance: addressing the COVID-19 pandemic panopticon, *International Labour Review* Vol. 161, No. 2 (2022), pp. 289–315.

Aloisi, Antonio and Gramano, Elena, Artificial intelligence is watching you at work: digital surveillance, employee monitoring, and regulatory issues in the EU context comparative, *Labor Law & Policy Journal* Vol. 41, No. 1 (2019), pp. 95–122.

Auer-Mayer, Susanne, Dürfen Arbeitnehmer*innen im "Home-Office" überwacht werden?, CuRe 2020/88.

Felten, Elias and Preiss, Jochen, *§ 96a ArbVG*, in: Gahleitner, Sieglinde and Mosler, Rudolf (eds), *Arbeitsverfassungsrecht* 3[6], ÖGB-Verlag: Wien, 2020, pp. 230–249.

Goricnik, Wolfgang, *Art 88 DSGVO*, in: Knyrim, Rainer (ed), *DatKomm*, Manz Verlag: Wien, 2023, pp. 1–63.

Goricnik, Wolfgang, Wider das "Trojanische Pferd" home-office im Dauerrecht, *DRdA-infas* Vol. 2 (2021), pp. 149–152.

Jervis, Claire E. M., Barbulescu v Romania: Why there is no room for complacency when it comes to privacy rights in the workplace. *Industrial Law Journal* Vol. 47, No. 3 (2018), pp. 440–453.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010

Kotschy, Waltraut, Article 6 Lawfulness of processing, in: Kuner, Christopher et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic: New York, 2020, pp. 321–344.

Krause, Rüdiger, Sozialverträgliche Arbeitnehmerüberwachung – Technikbasierte Beschäftigtenkontrolle als Gegenstand betrieblicher Mitbestimmung im digitalen Zeitalter, in: Gräfl, Edith, Lunk, Stefan, Oetker, Hartmund and Trebing, Yvonne (eds), *100 Jahre Betriebsverfassungsrecht*, CH Beck Verlag: München, 2020, pp. 353–369.

Molè, Michele and Mangan, David, 'Just more surveillance': The ECtHR and workplace monitoring. *European Labour Law Journal* Vol. 14, No. 4 (2023), pp. 694–700.

Nurse, Jason R. C., Williams, Nikki, Collins, Emily, Panteli, Niki, Blythe, John and Koppelman, Ben, Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy, in: *23rd International Conference on Human-Computer Interaction*, 24–29 Jul 2021, pp. 1–8.

Van Eecke, Patrick and Šimkus, Anrijs, Article 88 Processing in the context of employment, in: Kuner, Christopher et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford Academic: New York, 2020, pp. 1229–1239.

Vitak, Jessica and Zimmer, Michael, Surveillance and the future of work: exploring employees' attitudes toward monitoring in a post-COVID workplace. *Journal of Computer-Mediated Communication* Vol. 28, No. 4 (2023), pp 1–11.

WP29 2017: Article 29 Working Party, 'Opinion 02/2017 on Data Processing at Work' (WP 249, 8 June 2017).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 17:07:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009597029.010