Automated Monitoring in the Workplace and the Search for a New Legal Framework: Lessons from Germany and Beyond

Halefom Abraha

Abstract

Workers have specific data protection needs that cannot be addressed by general data protection rules. The GDPR was never designed to adequately handle these specific issues; it was designed under the assumption that data processing in the employment context would be regulated by a separate set of rules. The introduction of such specific rules has been debated for a long time but with little progress. Instead, a closer look at the policy and regulatory debate on the need for separate employee data protection legislation in Europe shows that the increasing calls from stakeholders for separate employee data protection legislation have been met by legislative inaction both at the Union and Member State levels. This paper explores the persistent policy gap in regulating employee data processing in the EU. It argues for the urgent need for independent legislation by Member States to address the challenges posed by new monitoring and algorithmic management systems to workers’ privacy and data protection rights.

The paper builds on recent developments in Germany that can offer useful lessons—and serve as a cautionary tale for other Member States. The significant political momentum in Germany towards adopting workplace data protection legislation presents an opportunity for other Member States to follow suit. At the same time, the fact that the German rules regulating employee data processing were recently pronounced by the CJEU as incompatible with the GDPR should serve as a cautionary tale. The paper then provides guidelines for Member States on using the facultative clause under Article 88 of the GDPR to introduce independent employee data protection legislation and outlines key policy proposals for such legislation.

Keywords: GDPR, Article 88, labour law, employee monitoring, algorithmic management, workplace data protection, privacy, CJEU

1. Introduction

Workforce monitoring is an inherent employer prerogative. The question at the heart of regulating employee data processing is thus not whether, but the extent to which such monitoring is justifiable. Drawing that boundary, however, has become more challenging as employers increasingly take advantage of technological advances, taking employee monitoring and surveillance to the next level. These technologies and practices give rise to novel legal questions or at least questions that do not have an explicit answer in existing regulatory regimes. The GDPR, for instance, is not adequate to address the unique features of the employment relationship (such as the relationship of proximity and dependence) as the Regulation was designed under the assumption that data processing for employment purposes would be regulated by a different set of rules. Specifically, the GDPR recognises that workers have specific rights to dignity and privacy that cannot be addressed by omnibus data protection rules.
However, previous research shows that such employment-specific data protection rules are not yet developed across the EU.\(^1\) Because of this legislative inaction, courts and national authorities are grappling with how to interpret general data protection rules in the employment context. The existing rules are interpreted and enforced inconsistently, creating legal uncertainty for employers and employees alike. Recent developments in Germany illustrate the challenges in regulating employee data processing and expose the cracks in the existing rules.

On 9 February 2023, the Hanover Administrative Court in Germany ruled that the constant and real-time monitoring of workers at Amazon’s logistics centre was lawful, overruling a decision made by the Lower Saxony State Data Protection Commissioner (DPC).\(^2\) The Administrative Court determined that Amazon’s practice of using hand scanners to monitor every movement of employees while performing their work satisfied the data protection requirements pursuant to Article 88 of the GDPR in conjunction with Section 26(1) of the German Federal Data Protection Act (BDSG).\(^3\) Contrary to the DPC’s assessment, the court argued that Amazon’s corporate interests outweighed workers’ privacy and data protection rights.

Interestingly, two months later, the Court of Justice of the European Union (CJEU) suggested that the relevant provisions of the BDSG, which the Hanover Administrative Court had relied upon, were incompatible with Article 88 of the GDPR and therefore inapplicable. In response to a request for a preliminary ruling from the Administrative Court of Wiesbaden, the CJEU found that the German legislation regulating personal data processing in the employment context does not qualify as ‘more specific rules’ for the purpose of Article 88 GDPR.\(^4\)

These contradicting decisions come amid repeated calls and mounting pressure on the German legislature to introduce independent employee data protection legislation, separate from the general rules of the BDSG. While the German legislature has been reluctant to take these calls seriously, the recent developments could make such legislative inaction unsustainable. However, the problem is not unique to Germany. While the GDPR creates an opportunity under Article 88 for the Member States to introduce independent employee data protection laws, few have done so.

Drawing on the recent developments in Germany, this paper maps the persistent policy gap in regulating employee data processing in the EU and argues for the urgent need for independent legislation to address the privacy and data protection risks posed by new employee monitoring and algorithmic management systems. It then articulates what such independent legislation should look like substantively by identifying key policy proposals.

Discussion proceeds in three parts. The next section provides a brief overview of how an increasing number of employers are leveraging new automated monitoring and decision-making technologies, which have significant ramifications for workers. It then identifies the recurring regulatory challenges and traces the evolution of the policy debate on regulating employee data processing over time. This debate, however, has encountered legislative inaction.

Section 3 draws lessons from recent developments in Germany. On the one hand, there is significant political momentum in Germany towards adopting workplace data protection

---


\(^2\) Regional Administrative Court of Hannover, Case 10 A 6199/20 February 8, 2023.

\(^3\) ibid 53–58.

\(^4\) Case C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums ECLI:EU:C:2023:270.
legislation. On the other hand, the CJEU recently pronounced that the German rules regulating employee data processing are incompatible with the GDPR. Section 4 makes the case for independent employee data protection legislation. It provides guidelines for Member States on utilising Article 88 of the GDPR to introduce independent employee data protection legislation and outlines key policy proposals for such legislation. The final section offers a conclusion.

2. Automated Employee Monitoring and the Regulatory Gap

Employers increasingly use electronic monitoring to track their workers’ every move and predict a wide range of worker behaviours. New automated monitoring and algorithmic management technologies ‘enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles and wearables.’ These technologies continue to grow with the increasing datafication of the workplace. Industry and media reports show that the global demand for employee monitoring tools increased dramatically following the COVID-19 pandemic and continues to grow with no sign of slowing.

Workers tend to be aware of the fact that their activities and behaviours in the workplace are subject to some sort of monitoring. However, they ‘do not abandon their right to privacy and data protection every morning at the doors of the workplace.’ Workers expect that their workplace privacy and data protection rights are balanced with the employer’s legitimate interests. While employers have a range of legitimate interests to monitor their workforce and utilise new technologies to do so, such monitoring cannot reduce the privacy and data protection rights of workers to zero.

Therefore, the recurring and complex policy question is the extent to which such monitoring is justifiable. This question is particularly pressing as new automated monitoring and decision-making technologies become commonplace across the economic spectrum. Kirstie Ball identifies three examples where employee monitoring and surveillance can become problematic: (i) when employee monitoring goes far beyond what is necessary and proportionate for business interest, (ii) when the collection of personal data concerning employees goes beyond what is necessary for the performance of their contract, and (iii) when monitoring affects existing levels of control, autonomy and trust. New automated monitoring technologies have intensified these three causes of controversy.

First, what constitutes ‘necessary and proportionate’ employee monitoring remains uncertain, context-dependent, and prone to abuse. It changes over time, in different contexts, and across business models. Employers can easily argue that any form of monitoring and surveillance in the workplace is proportionate and necessary for the business interests and purposes they define themselves, including improving productivity, efficiency, and innovation.

5 Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017 9.
7 This does not mean that workers know the extent to which they are being monitored in the workplace.
9 Bărbulescu v Romania [2017] ECtHR 61496/08 [80].
10 Ball (n 6) 10–11.
New technologies such as automated monitoring and algorithmic management tools exacerbate this problem by creating new sources of data, new insights, and new ways of control, including predicting and directing or influencing workers’ future behaviour. Most importantly, the collection and processing of massive quantities of worker personal data have become more essential to most businesses, which incentivises employers to resort to more intrusive monitoring practices beyond what is necessary for business interests. Employers could use this data to produce value in a way incompatible with pre-defined business purposes. This development also blurs the boundaries of business-related information and the personal data of employees. Further complicating things, the fact that workers’ personal data becomes increasingly embedded with business-related information means that such personal data could be subject to corporate interest and trade secret claims. In some extreme scenarios, employers can use the personal data they collect on workers’ behaviour to predict and quash the likelihood of workers exercising their legal rights, such as the right to organise. Therefore, expecting employers to restrict their monitoring and surveillance powers to the bare minimum is implausible. On the other hand, without clear guardrails in place, employers are likely to continue to deploy automated monitoring and decision-making technologies in ways that significantly harm workers’ fundamental rights.

Second, the extent to which employees are monitored is no longer limited to performance management: workers’ thoughts, feelings and physiology can equally be tracked and analysed, and their behaviour predicted. As Charlotte Garden has pointed out, employee monitoring technologies collect a wide range of different types of personal data in the workplace, including data on ‘whom [workers] talk to, what they type, how quickly they complete tasks and even their mood’. As illustrated in the figure below (see Figure 1), vendors do not shy away from advertising the monitoring tools that they are capable of tracking and analysing virtually everything and anything that is technically possible.

---

14 Ball (n 6).
Third, it is extensively documented in the literature and media reports that employers use invasive employee monitoring and automated decision-making tools in such a way as to negatively affect workers’ control over their work, and their human dignity and autonomy, and erode workplace trust and morale. Making things worse, some of the most invasive employee monitoring tools can be deployed remotely and secretly monitor workers’ every move and activity on their devices, including secretly activating webcams and microphones. Interestingly, some of the key players in the employee monitoring market, such as ‘InterGuard’ and ‘iMonitorSoft’, advertise secret monitoring and profiling capabilities as a selling point. For instance, iMonitorSoft suggests that its ‘All-In-One Employee Computer Monitoring Software’ ‘is running in total stealth mode […] it can secretly monitor employees. The software is not visible in the system tray, desktop, system processors or other areas of the computer.’ What is more worrisome than the capability of such monitoring software is the existence of a market for it.

Unrestrained employee monitoring and surveillance practices could do more harm than good to employees and employers alike. Beyond privacy and data protection harms, these practices pose unprecedented challenges to the human dignity, legitimate interests and other fundamental rights of workers. For instance, new monitoring and decision-making technologies could normalise extensive surveillance; exacerbate information, knowledge, and power asymmetries in the workplace; and deteriorate working conditions, leading to

---

16 Employee Monitoring Software for Telework’ (InterGuard, 17 April 2020) <https://web.archive.org/web/20200417052503/https://www.interguardsoftware.com/employee-monitoring-software/> accessed 25 July 2023. This practice could be illegal in some jurisdictions such as the EU.
permanent pressure on workers to adapt and perform and exposing them to several psychosocial risks. Furthermore, new monitoring and surveillance technologies enable employers to predict the future behaviours of workers and ‘pre-emptively pick out employees who are most likely to engage in union organizing, talk to journalists, protest stagnation in pay, or even quit their jobs’.  

Unregulated employee monitoring and surveillance could also be counterproductive, incentivising behaviours opposite to what such practices aim to achieve. For instance, intrusive monitoring of workers could catalyse resistance, incentivise workers to subvert or break workplace rules, fuel unionising and worker organising, decrease job satisfaction and organisational commitment, increase turnover propensity, erode organisational trust, and decrease fairness and justice perceptions.  

However, this does not mean that these technologies do not have benefits for workers. If implemented in the right way, new monitoring and decision-making tools can be used in a way that benefits both workers and employers. As the Eurofound noted, for instance wisely implemented employee monitoring and surveillance systems can be used for legitimate purposes that benefit workers by ‘facilitating skills development and on-the-job learning’, ‘ensuring workers’ safety, especially in hazardous or emergency situations’ and by ‘improving productivity, workplace practices and working conditions’. Therefore, a properly designed and adequately enforced regulatory framework stands to benefit both employers and workers alike. Regrettably, such regulatory frameworks are not yet developed across the EU.

The issue of privacy and data protection in the workplace has been debated at the EU and Member State level since the 90s. Based on the key issues of concern, the progress of the policy debate since then can generally be classified into three phases.

The first phase is the pre-GDPR era (1999-2012). During this period, the main concern of privacy and data protection law in the employment context was the extent to which the

---

25 Ball (n 6).
26 Sara Riso, ‘Monitoring and Surveillance of Workers in the Digital Age’ (Eurofound) <https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age> accessed 3 October 2023 [Noting that ‘wearables (…) can be used to benefit employees by facilitating the acquisition of new skills or making it possible to perform challenging tasks under the supervision of a more experienced worker’].
27 Outside the EU, the Council of Europe and ILO introduced ‘Recommendation on the Protection of Personal Data Used for Employment Purposes’ in 1989, and the Code of Practice on the Protection of Workers’ personal data’ in 1997, respectively.
employer could monitor employees’ private electronic communications (specifically telephone, internet access, and email communications) in the workplace. Two policy initiatives undertaken during this period are worth noting. The first policy initiative was the European Commission’s two-stage consultation on the protection of workers’ personal data with social partners launched in 2001 and 2004. While the Commission was of the opinion that a European framework was ‘needed aiming at the protection of workers’ personal data while striking a balance between the employer’s legitimate interests and the workers’ right to privacy’, the initiative was dropped for lack of consensus among stakeholders. Another policy intervention was the European Union’s Article 29 Working Party’s (WP29) Opinion 8/2001 on the processing of personal data in the employment context. This Opinion was complemented by a ‘working document’, which singled out ‘e-mail monitoring and surveillance of Internet access’ in the workplace as a primary concern.

The years 2012-2018 constitute the second phase, in which the GDPR was debated and finalised. This phase started with the Commission’s announcement in 2012 of its proposal to introduce a comprehensive ‘omnibus’ framework unifying data protection law across the Union and culminated with the entry into force of the GDPR in 2018. The focus of policy debates evolved, going beyond mere surveillance and monitoring: emphasis was increasingly placed on the ‘datafication’ of the workplace more generally. The concern was that almost everything (every behaviour, and practice in the workplace) could be transformed into digital data and that the monitoring and analysis of this data by employers would transform the power dynamics in the workplace, posing significant risks to human dignity, legitimate interests and fundamental rights of employees. The Commission attempted to respond to these concerns by contemplating the introduction of ‘detailed and harmonised rules for [the] employment relationship’ as part of the GDPR. In this regard, three notable issues were considered in the preparatory work leading to the adoption of the GDPR: (i) the introduction of detailed rules on the ‘proportionality and legitimacy’ requirements of personal data processing in the employment context, (ii) the clarification of consent as a valid legal basis for the processing of workers’ personal data, and (iii) the provision of a delegated power to the Commission to provide for specific rules for the purpose of further specifying the criteria and requirements for the safeguards of personal data in the employment context. Unfortunately, none of these efforts made it into the GDPR.

The policy debate after the entry into force of the GDPR (2018-present) can be described as the third phase. Today, the primary concern is the ubiquitous deployment of artificial intelligence and algorithmic management tools in the workplace and the risks they pose to

---

28 See, for instance, Bărbulescu v. Romania (n 9) para 80. The case originated in an application lodged on 15 Dec 2008.
30 ibid; For more details on this, see Abraha, ‘A Pragmatic Compromise?’ (n 1).
32 WP29 (n 8).
35 ibid 47.
36 ibid 19.
37 Article 82(2) draft GDPR, COM(2012) 11 final.
38 For a detailed analysis of why the EU failed to harmonise data protection rules in the employment context, see Abraha, ‘A Pragmatic Compromise?’ (n 1).
employees. It is (perhaps unsurprisingly) hard to find EU policy documents during the previous two phases that discussed artificial intelligence and algorithmic management in the employment context. For instance, neither the legislative proposal which was to become the GDPR nor its accompanying impact assessment mentioned these issues.

These three phases demonstrate that the issue of regulating data processing in the employment context has become increasingly complex over time – from monitoring private electronic communications to datification to algorithmic management and artificial intelligence. The more employers take advantage of new technological advances, the more complicated and intractable the regulatory challenges have become. This is because these advanced technologies give rise to novel regulatory challenges and exacerbate existing ones.

The regulatory challenges exist both at the supply chain and operational levels. The regulatory gaps at the supply chain level exist because the automated monitoring and decision-making tools used in the workplace are most often developed, provided, and controlled by third-party vendors (not by the employers themselves). These third-party vendors operate in a largely unregulated environment. For instance, AI developers and providers are operating in a regulatory vacuum (with no oversight and accountability mechanisms), though policymakers have started to take note of the need to tackle the problem. Compounding this regulatory vacuum, the software industry is highly centralised, and the automated monitoring and decision-making tools are standardised. For instance, some industry studies show that over one-third of the Fortune 100 companies use the same automated candidate screener AI, developed by a company called HireVue.

Several problems also arise at the operational level that current regulatory regimes are ill-suited to address. For instance, as highlighted above, the GDPR has a design problem in addressing the risks posed by advanced monitoring and decision-making systems in the workplace. The GDPR also faces an enforcement crisis in the employment context with most national data protection authorities lacking the legitimacy, interest, expertise, and resources to do their job.

Despite these gaps, the EU and the Member States are yet to introduce regulatory frameworks that fit these challenges. In its first report on the evaluation and review of the GDPR issued on 24 June 2020, the Commission suggested that more guidance was needed on the employment context. To date, no such guidance has been issued. Therefore, after decades of debate and despite the profound changes in the workplace as a result of digitalisation, there is currently no EU data protection law that exclusively regulates data processing in the employment context.

Member states have also missed the opportunity created under Article 88 GDPR. Recognising that employee data protection is a unique sub-field of data protection law, the EU

39 The past few years have seen the proliferation of AI regulatory initiatives around the world that would make AI developers and providers responsible for their products. In the EU context, for example, the most widely debated is the proposed AI Act. However, the proposed AI Act does not have specific protections for workers. See Paul Soler, ‘EU Workers’ Rights Missing from Landmark AI Law’ (EUobserver, 19 June 2023) <https://euobserver.com/digital/157163> accessed 6 September 2023.


41 see Justin Nogarede, ‘No Digitalisation without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace’ (FEPS Policy Study, November 2021); Abraha, ‘A Pragmatic Compromise?’ (n 1).

42 Communication from the commission {SWD(2020) 115 final}.

43 Although it is the non-binding WP29 Opinion 2017 remains the only concrete policy document, it was prepared largely based on Directive 95/46/EC.
legislature has given the Member States the opportunity to enact independent legislation that exclusively regulates employee data processing. Regrettably, the facultative clause stipulated under Article 88 GDPR remains underutilised, or at least improperly utilised. Despite the opportunity created under this provision, few Member States have introduced such specific legislation. Existing Member State data protection laws in the employment context are, at best, patchy, inadequate, and inconsistent.

The consequence is that courts and national authorities are grappling with how to interpret general data protection rules in the employment context. Existing rules are interpreted and enforced inconsistently, creating legal uncertainty for employers and employees alike. Recent developments in Germany illustrate the challenges in regulating data processing in the employment context and expose the gaps in the existing rules.

3. Lessons from Germany

Germany is one of the Member States that has enacted national legislation utilising Article 88 GDPR. However, the German legislation has been criticised for failing to provide adequate protections for workers and was recently pronounced by the CJEU as incompatible with the GDPR. The recent CJEU judgment has reinforced the repeated calls on the German legislature to introduce comprehensive and freestanding workplace data protection legislation.

The developments in Germany could offer a useful lesson and serve as a cautionary tale for other Member States. The fact that significant political momentum has developed in Germany to adopt independent workplace data protection legislation could open the opportunity for other Member States to follow suit. German law has had a fundamental impact on shaping data protection rules in general, and it is likely to play a similar role in employment-specific data protection law. At the same time, the fact that legislatures both at the federal and state levels in Germany have improperly utilised Article 88 of the GDPR should serve as a cautionary tale.

A. Ambivalent Regulatory Approach

The need for independent employee data protection legislation in Germany has been debated for a long period of time and remained unsettled (see table 1 below). The first German data protection law introduced in 1990, did not have any employment-specific provisions. The only provision for employee data protection was introduced for the first time as part of the amended Federal Data Protection Act in 2009. Section 32 of this Act, which exclusively dealt with employee data processing, was included as a response to a series of employee surveillance scandals uncovered during that time. This provision was never sufficient to address the special features of employee data processing and was subjected to several criticisms. Repeated calls and attempts since then to introduce an independent employee data protection law have

44 See Valerio De Stefano, ‘AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU’s Legal Framework’ (European Parliamentary Research Service, PE 729516 2022); Abraha, ‘A Pragmatic Compromise?’ (n 1); Nogarede (n 41).
45 Abraha, ‘A Pragmatic Compromise?’ (n 1).
46 The Federal Data Protection Act was introduced in response to the census ruling by the Federal Constitutional Court in 1983, which laid down the foundation for the right to informational self-determination.
never materialised.\textsuperscript{49} For instance, a ‘Draft Employee Data Protection Act’ proposed for the legislative period 2009-2013 did not lead to results due to a lack of consensus.\textsuperscript{50}

The German legislature also missed the new opportunity created by the GDPR. The GDPR required Member States to amend domestic rules and created the opportunity for introducing a separate law on employee data protection. However, instead of creating an independent and comprehensive employee data protection law, the German federal legislature introduced Section 26 of the new Federal Data Protection Act 2017 (BDSG), which maintained the pre-GDPR general rules with slight modification.\textsuperscript{51} There was no agreement on using Article 88 of the GDPR to create separate and comprehensive employee data protection law. As Lukas Middel aptly pointed out, ‘this was not a great step forward by the legislature’.\textsuperscript{52} As a result, the BDSG 2017 (last amended 2021) has been criticised by scholars and policymakers for failing to provide specific and adequate measures that safeguard the right of employees to the protection of their personal data.\textsuperscript{53}

At the same time, the calls and efforts for separate legislation have continued. The coalition agreement for the legislative period 2017-2021 suggested using Article 88 GDPR to establish a new employee data protection law. This was followed by the creation of the ‘Data Ethics Commission’, which recommended the Federal Government ‘invite the social partners’ to develop a new employee data protection law.\textsuperscript{54} The Advisory Council on Employee Data Protection established by the Federal Ministry of Labor (BMAS)\textsuperscript{55} also reached the same conclusion: an independent Employee Data Protection Act was needed. In its final report released in January 2022, the Council’s report specifically pointed out that the federal legislature must use the opportunity under Article 88 GDPR.\textsuperscript{56} Trade unions and data protection authorities have also raised their voices. The German Trade Union Confederation (DGB) went to the extent of drafting new legislation\textsuperscript{57}, while the Data Protection Conference (DSK) issued two resolutions emphasising the urgency for independent employee data protection law.\textsuperscript{58} There is a consensus among these stakeholders regarding the need for additional employee data protection.

\begin{footnotes}
\item[49] Lukas Middel, ‘Workplace Surveillance in the Light of Employee Data Protection’ (Expert opinion for the Center for Interdisciplinary Labour Law Studies, Law Faculty, Europa-Universität Viadrina, Frankfurt (Oder), Germany 2019).
\item[50] For details on the controversies about this proposal, ibid.
\item[51] The requirements for processing employee personal data remain largely the same under the new BDSG as the previous law. The main difference between Sec. 32 of the old Federal Data Protection Act 2009 and the BDSG 2017 is that the latter added ‘collective agreements’ as a legal basis to process employee data processing.
\item[52] Middel (n 49) 5.
\item[54] ‘Gutachten Der Datenethikkommission’ (2019) <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?fileId=DC070CBAF42A76936D70D683117C1DA3.1_cid373?__blob=publicationFile&v=7>.\textsuperscript{55}
\item[56] ‘German BMAS Publishes Independent Advisory Board’s Employee Data Protection Recommendations’ (n 53).
\end{footnotes}
protection rules. Common themes highlighted in the documents include the necessity of clarifying the role of consent, establishing specific rules for data processing based on collective agreements, imposing restrictions on behavioural and performance control, and establishing specific rules concerning artificial intelligence. Interestingly, in the draft employee data protection legislation DGB, less emphasis is given to artificial intelligence compared to the other initiatives.

<table>
<thead>
<tr>
<th>Timeline</th>
<th>Key policy development</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1983</td>
<td>Census ruling</td>
<td>Laid down the foundation for the right to informational self-determination</td>
</tr>
<tr>
<td>1990</td>
<td>The first Federal Data Protection Act adopted</td>
<td>It was a response to the Census ruling, No employment-specific provision was included</td>
</tr>
<tr>
<td>2009</td>
<td>Federal Data Protection Act amended</td>
<td>An independent provision (sec 32) for employee data protection was introduced for the first time, It was a response to many employee surveillance scandals uncovered by the press in 2005.</td>
</tr>
<tr>
<td>2009-2013 (Leg. period)</td>
<td>SPD (opposition parties) proposed a Draft Employee Data Protection Act</td>
<td>Legislative project was never realised because of a lack of consensus.</td>
</tr>
<tr>
<td>2017</td>
<td>New Federal Data Protection Act (BDSG) adopted</td>
<td>This was because of the GDPR’s requirement to make necessary amendments to national laws, Section 26 (amendment to old Sec 32) introduced, using Art. 88 GDPR, Was not possible to agree on using Art 88 to create separate/comprehensive employment-specific legislation, Sec 26 was a minimum consensus and not substantially different from old Sec 32</td>
</tr>
<tr>
<td>2017-2021 (Leg. period)</td>
<td>Coalition agreement indicated making use of Art 88 and establishing a separate law of employee data protection</td>
<td>The Data Ethics Commission was set up, The Commission released its report in 2019 recommending the Federal Government invite social partners to develop a common line for legal specifications of employee data protection.</td>
</tr>
<tr>
<td>2020</td>
<td>The Federal Ministry of Labor established an Advisory Council on Employee Data Protection (BMAS)</td>
<td>Mandated to examine whether an independent law on employee data protection should be enacted</td>
</tr>
<tr>
<td>January 2022</td>
<td>BMAS released its detailed final report</td>
<td>BMAS concluded independent Employee Data Protection Act is necessary using Art. 88</td>
</tr>
<tr>
<td>Feb 2022</td>
<td>German Trade Union Confederation (DGB) presented a draft law for an employee data protection law</td>
<td>Central issues of the draft include consent, AI, behaviour monitoring, consent, information rights of employees</td>
</tr>
<tr>
<td>April 2022</td>
<td>The Data Protection Conference (DSK) issued a resolution on employee data protection.</td>
<td>Emphasised the urgency for independent law, Recommended independent employee data protection law to focus on key areas including AI, behaviour monitoring, consent, and collective agreement.</td>
</tr>
<tr>
<td>Feb 2023</td>
<td>The Administrative Court of Hanover ruled in favour of Amazon</td>
<td>Found constant monitoring of employees practised by Amazon to be lawful, The Court assumed that the national law (Sec. 26 BDSG) based on which personal data was processed was in conformity with the requirements of Art 88</td>
</tr>
</tbody>
</table>
The above analysis shows a familiar trend in Germany: the increasing calls by stakeholders for separate employee data protection legislation have been met by legislative inaction. However, recent developments could make such legislative ambivalence unsustainable. Two recent court decisions and a CJEU pending case have particularly made the status quo untenable and the need for new law more urgent.

B. Hanover Administrative Court Judgment on Employee Monitoring by Amazon

Amazon, which has a reputation for intrusive surveillance and inhumane working conditions, requires employees at its logistics centre in Winsen to use hand scanners. These scanners monitor every movement of every employee when performing their work. The data collected by means of the hand-held scanners in real-time is stored and evaluated with the performance management software ‘Fulfilment Center Labor Management’ (FCLM). Based on the data collected by FCLM on a constant and minute-by-minute basis, another software called ‘Associate Development and Performance Tracking’ (ADAPT) evaluates the work performance data and creates performance profiles for each employee. ADAPT serves two interrelated purposes: (1) it automatically generates performance feedback and notifies all employees once per quarter, and the best-performing 10% and least-performing 5% every two weeks, and (2) it sends auto-generated feedback to area managers to be used as a basis for personnel decisions including promotions and dismissals.

In 202n, the Lower Saxony State Data Protection Commissioner (DPC) found that Amazon’s practices constituted a serious interference with the right to informational self-determination without justification and was thus unlawful. Amazon’s data processing, the DPC suggested, did not meet the requirements of lawfulness, necessity, and proportionality under the GDPR.

Amazon argued that the collection of personal data was indispensable to protect substantial legitimate interests, specifically to control the logistics processes, to control the individual qualification of employees, and to create objective assessment bases for individual feedback and personnel decisions.

While recognising Amazon’s legitimate interest, the DPC was not convinced that the uninterrupted collection of current and minute-by-minute performance data of the employees was necessary to achieve that purpose. The DPC argued that the company had failed to show that ‘the processing was unavoidable in order to achieve the purpose’. The DPC then pointed

---

59 Greene (n 24).
60 VG Hannover (n 2).
61 ibid 20.
62 Amazon argued that the legal basis for the data processing in question was Article 6(1)(f) of the GDPR (in addition to Section 26 of the BDSG).
63 VG Hannover (n 2) para 35.
out various approaches to data processing that would interfere less intensively with the right to informational self-determination of the employees.64

Even assuming that the data processing was necessary to achieve legitimate purposes, the DPC reasoned that the interference with the privacy rights of the employees was ‘disproportionate’65:

- The comprehensive collection of personal data carried out by [Amazon] constituted a case of total surveillance of the employees working in the logistics centre.66
- The continuous collection of performance data led to permanent pressure on the employees to adapt and perform (because personnel measures such as promotion depend on performance data).67
- Amazon failed to provide evidence that the data processing did not in fact create any monitoring pressure on the employees.68

Based on the above considerations, the DPC concluded that the fundamental rights of the employees outweighed the business interests of the company. In other words, Amazon could not base its data processing on Article 6(1)(f) of the GDPR. The DPC then instructed Amazon to cease the continuous collection and analysis of data by means of the specialised applications FCLM and ADAPT beyond the period of three months after the establishment of the employment relationship.69

The Hanover Administrative Court disagreed with the DPC’s assessment and overruled the decision. The administrative court rejected the orders issued by the DPC as substantively unlawful, disproportionate, and not suitable to protect employees’ right to informational self-determination. The court found the data processing to be lawful for three reasons. First, the court held that the legal basis for data processing was Article 88 (1) of the GDPR in conjunction with Section 26 (1) sentence 1 of the BDSG.70 The court then went on to argue that Section 26 (1) sentence 1 BDSG is lex specialis to Article 6(1)(f) of the GDPR and the former prevails over the latter insofar as employee data protection is concerned.71 Second, the court found the data processing to be necessary to achieve the legitimate purposes put forward by Amazon. Contrary to the DPC’s assessment, the court was not convinced that a milder, equally effective means was available to achieve these interests. Third, the court held that the interference with the right to privacy of the employees was not disproportionate.

Amazon’s data processing furthermore met the proportionality test, not least as

- the intensity of the data collection was not unduly high and the employees are not unduly burdened by it,

64 ibid 20, 80.
65 ibid 20,38.
66 ibid 38.
67 ibid 20.
68 The DPC was not convinced by Amazon’s claim that ‘the data processing had no negative consequences for the employees’. ibid 38.
69 ibid 18–19. The DPC initiated its data protection monitoring procedure on 27 November 2017 and delivered its final decision on 28 October 2020.
70 Section 26 (1) sentence 1 BDSG justifies data processing of employees’ personal data, inter alia, if the data processing is necessary for the performance of the employment relationship.
71 ‘Insofar as section 26 BDSG contains legal bases, the provisions of the GDPR (Art. 6(1)b, f) take a back seat (section 26 (1) sentence 1 BDSG is lex specialis to these GDPR provisions.’
- the employees were aware of how, by whom and for what purposes the data was processed,
- the data processing did not have excessively serious consequences on the employees, and
- no special categories of data were collected.

The Hanover Administrative Court decision is deeply problematic on at least three grounds. First, because the national court assumed that the national law based on which personal data was processed was in conformity with the requirements of Article 88 of the GDPR. This is not entirely correct, as the CJEU subsequently reasoned in Case C-34/21. If the CJEU judgment was delivered earlier, the administrative court would likely have reached a different conclusion, as implied in its reasoning.\textsuperscript{72} As regards the proportionality analysis, the court took Amazon’s argument almost at face value. The court concluded that Amazon’s legitimate interests, which can be boiled down to ‘efficiency’, for example, meeting the delivery dates guaranteed to customers,\textsuperscript{73} outweighed the rights and freedoms of the employees. The court appeared more concerned with the company’s economic interests than its workers’ privacy rights. As the DPC pointed out, this approach could render compliance with data protection law in the workplace into ‘mere lip service’.

Second, the court downplayed the negative impact of uninterrupted monitoring on employees. The court rejected the ‘decisive factor’ for the DPA’s decision that the data processing created ‘a permanent pressure to adapt and perform’ on the employees. On the contrary, the court was of the opinion that the decisive factor must be ‘which consequences [were] attached to the collected data’. In this regard, the court agreed with the DPC that permanent pressure to adapt and perform would be created for fixed-term employees because the performance was used as a basis to extend or terminate their contracts. However, this did not affect the court’s decision. Furthermore, the court did not expect that permanent employees would be exposed to permanent pressure to adapt and perform. This reasoning ignores the mounting evidence produced by investigative reports, journalistic work and academic research that excessive employee monitoring has multifaceted and far-reaching negative consequences for workers. In fact, similar monitoring and strict productivity tracking practised by Amazon in other logistics centres are often characterised as excessively intrusive and dehumanizing.\textsuperscript{74} Ignoring these reports, the court suggested that permanent monitoring could have a positive impact on employees, including reducing stress.

Even more interestingly, finally, the court seemed to perceive the automated performance tracking and performance evaluation systems (FCLM and ADAPT) used by Amazon to be infallible and unbiased. The court accepted Amazon’s claim that these systems generate ‘objective and fair’ assessment bases for feedback and personnel decisions. This reasoning flies in the face of mounting evidence showing that algorithmic management tools used in the workplace are error-prone and can produce unfair and biased results. Furthermore, the fact that the feedback generated by Amazon’s algorithmic management systems is characterised as ‘objective and fair’ risks that human managers could defer their decisions— including terminating the employment contract— to the algorithms by simply relying on the automatically generated feedback.

\textsuperscript{72} The court noticed that a decision by the CJEU on the matter was imminent, but it nonetheless assumed that Section 26 of the BDSG was compatible with Article 88 GDPR.

\textsuperscript{73} From the perspective of the DPC, Amazon could achieve the goal of delivering packages on time even without individual performance monitoring. For example, it is conceivable that only the location of a good within the logistics centre is tracked.

\textsuperscript{74} Zarook (n 21); Greene (n 24).
This case shows a familiar trend in Germany in that courts and DPAs have taken different paths in which DPAs have often taken more protective decisions and interpretations than courts. However, the problem goes beyond the court’s assessment of the facts and interpretation of the law. Part of the problem has to do with the way the existing rules regarding data protection in the workplace are designed.

C. The CJEU on the Compatibility of German Employee Data Protection Rules with the GDPR

On 30 March 2023, the European Court of Justice (CJEU) ruled for the first time on the interpretation of Article 88 GDPR. In response to a request from the Administrative Court of Wiesbaden (Hauptpersonalrat der Lehrerinnen, Case C-34/21) concerning the live streaming of video classes, the CJEU found the German law regulating personal data processing in the employment context to be incompatible with the GDPR. Specifically, the relevant provisions of the Hessian data protection legislation on employee data processing (and, by extension, parallel domestic rules at the federal and state level in Germany) are neither sufficiently specific nor compatible with, EU law. The legislation does not flesh out any substantive ‘suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights’, hence failing to fulfil the conditions laid down in Article 88(2) GDPR. By extension, this means the employment-specific provisions of the Federal Data Protection Act (BDSG) and parallel rules at the state level in Germany are also incompatible with the GDPR.

The judgment will have broad legal and policy reverberations across the Union, especially for Member States with similar data protection laws. If evaluated against the criteria articulated by the CJEU in Hauptpersonalrat der Lehrerinnen, most Member State rules would likely fail to qualify as ‘more specific rules’.

Although the CJEU’s judgment is confined to the scrutiny of Paragraph 26(1) subparagraph (1) of the BDSG, the remaining parts of the provision are also called into question in a separate and pending preliminary ruling procedure initiated by the German Federal Labour Court (Bundesarbeitsgericht, BAG) (Case C-65/23- K GmbH). The BAG suggests that it cannot resolve the dispute in the main proceedings without first determining the interplay between the relevant national provision (Paragraph 26(4) of the BDSG) that allows for employee data processing based on ‘collective agreement’ and the GDPR.

The first question is of particular relevance for present purposes:

1. Is a national legal provision that has been adopted pursuant to Article 88(1) [and subject to compliance with Article 88(2) of the GDPR]—such as Paragraph 26(4) of [the BDSG] […] to be interpreted as meaning that the other requirements of [the GDPR] such as Article 5, Article 6(1) and Article 9(1) and (2) must always also be complied with?

---

76 For a detailed analysis of the CJEU judgment, see Halefom Abraha, ‘C-34/21 - Hauptpersonalrat v Wiesbaden: Article 88 GDPR and the Interplay between EU and Member State Employee Data Protection Rules’ Modern Law Review (forthcoming).
77 Case C-65/23 Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice (8 February 2023).
78 The issue in the main proceedings concerns, inter alia, a dispute on the lawfulness of data processing provided for and carried out under a particular works agreement concluded between the defendant (the employer) and a works council.
The relevant provision in question, Paragraph 26(4) of the BDSG, provides that ‘the processing of personal data, including special categories of personal data of employees, for the purposes of an employment relationship is permitted on the basis of collective agreements’ [emphasis added. The provision further stipulates that ‘the negotiating partners [are] to comply with Article 88(2)’ of the GDPR.

The BAG thus seeks to ascertain whether Paragraph 26(4) is to be considered sufficient in and of itself as a legal basis to the extent that no additional requirements of the GDPR need to be observed. A textual reading of the provision could give the impression that a collective agreement concluded pursuant to Paragraph 26(4) of the BDSG would, subject to compliance with Article 88(2) GDPR, render other additional requirements of the GDPR irrelevant. This could mean, for example, that employee-data processing would be permissible solely on the ground of a collective agreement even if the processing would not satisfy the requirement of necessity laid down in Paragraph 26(1) of the BDSG and Articles 5-9 of the GDPR.79

The BAG rejected, rightfully so, this line of interpretation as incompatible with the GDPR. In view of the BAG, compliance with the GDPR cannot be exempted by collective agreement.80 In other words, the fact that the rules for employee data processing are laid down by collective agreement does not make the relevant requirements of the GDPR inapplicable. Instead, ‘the ‘more specific provisions’ within the meaning of Article 88(1) […] – whether provided for by law or by collective agreements – will always also require compliance with the other requirements [of the GDPR].'81

It is conceivable that the CJEU would (and should) adopt a similar approach to Hauptpersonalrat der Lehrerinnen. In this regard, it is important to note that the opening clause under Article 88 should not be conflated with derogations and exemptions stipulated under different provisions of the GDPR. Article 88 of the GDPR is a ‘strengthening’ clause in that the ‘specific rules’ adopted within the meaning of Article 88(1) should complement and strengthen the general protections of the GDPR by providing special measures to safeguard human dignity, legitimate interests and the fundamental rights of employees. Therefore, the CJEU should answer the first question in the affirmative. It should ascertain that regardless of whether the legal basis for employee data processing is provided for by law or by collective agreements, the necessity requirements under Articles 5-9 of the GDPR must always also be complied with. This interpretation would ensure that collective agreements do not water down the level of protection of the GDPR.

Finally, the CJEU should also determine whether Paragraph 26(4) of the BDSG (i) qualifies as ‘specific rules’ and (ii) provides suitable and specific safeguarding measures, within the meaning of Article 88(1) and (2) respectively.82 In framing its first question, the BAG presupposes that Paragraph 26(4) of the BDSG is in conformity with Article 88 GDPR requirements.83 However, this would be unlikely considering the strict requirements identified by the CJEU in Case C-34/2. Paragraph 26(4) BDSG simply repeats the language of Article 88(1) without providing any specific rules and should therefore be interpreted as superfluous. The mere reference in Paragraph 26(4) sentence 1 of the BDSG to the fact that ‘the negotiating partners shall comply with Article 88(2)’ of the GDPR is only declaratory. Therefore, it is

79 Case C-65/23 Summary of the request for a preliminary ruling para 25.
80 ibid.
81 ibid 25.
82 The CJEU ruling in Case C-43/24 is confined to Paragraph 26(1) sentence 1 of the BDSG and does not address the issue of collective agreements.
83 In relation to its first question, the BAG also wants to know what is meant by ‘more specific rules’ within the meaning of Article 88(1) GDPR.
conceivable that the CJEU would reach the same conclusion as in C-34/21 and suggest that Section 26(4) BDSG is incompatible with Article 88 of the GDPR.

In conclusion, although Germany is one of the Member States that has enacted national legislation utilising Article 88 GDPR, the legislatures both at the federal and state levels got it wrong.\textsuperscript{84}

\section*{D. An Inflection Point?}

The German employee data protection landscape is at an inflection point. The profound changes in the world of work due to digitalisation pose unprecedented challenges to the human dignity, legitimate interests and fundamental rights of workers. At the same time, it appears that there is a growing political consensus on creating a new employment data protection law after several years of failed attempts. The recent developments (policy initiatives and court decisions) have also reinforced this favourable momentum. As Lower Saxony’s data protection commissioner, Barbara Thiel, pointed out after the Hanover Administrative Court’s judgment, ‘the ball is in the court of federal lawmakers’\textsuperscript{85} to respond by introducing new and comprehensive legislation that meets these challenges. Specifically, the CJEU judgment, pronouncing German regulations in the employment context incompatible with the GDPR, makes it all the more urgent for the federal legislature to step in and create separate employee data protection legislation. Even though the path to legislating employment-specific law in Germany seems a complex endeavour, the legislature may not have an option but to intervene.

\section*{4. The Case for Independent Employee Data Protection Law}

There are political, legal, and practical reasons why Member States should act and introduce independent data protection legislation. At the practical level, increasing digitalisation in the world of work poses unprecedented challenges to human dignity and workers’ fundamental rights. These challenges make the need for a legislative intervention all the more urgent. However, it seems that it is not politically feasible, at least in the short term, for the EU to introduce a comprehensive and harmonised employee data protection law. There are combinations of legal, political, and constitutional factors that have hindered efforts towards adopting harmonized employment-specific legislation at the Union level.\textsuperscript{86} The gaps in existing rules also justify the need for new employee data protection legislation. As highlighted above, the GDPR was never designed adequately to address the specificities of the employment relationship. It was designed under the assumption that data processing for employment purposes would be regulated by different, yet complementary, rules at the Member State level.\textsuperscript{87} At the same time, existing Member State laws are not adequate, and indeed may be incompatible with the GDPR as suggested in the recent CJEU judgment.

Given this state of affairs, it is time for the Member States to avail themselves of the opportunity created under Article 88 of the GDPR and introduce independent employee data protection laws that meet the special requirements of processing personal data in the workplace,

\textsuperscript{84} In its judgment in Hauptpersonalrat der Lehrerinnen the CJEU found that the Hessian data protection rules regulating employee data processing (and, by extension, parallel domestic rules at the federal and state level in Germany) are incompatible with the GDPR.
\textsuperscript{86} Abraha, ‘A Pragmatic Compromise?’ (n 1).
\textsuperscript{87} The GDPR is of course still relevant to the employment context and applies in its entirety to automated monitoring and decision-making so long as personal data processing is involved.
and specifically address the risks of new technologies such as algorithmic management. This section sketches out key elements of such regulation, taking into account the special features of the employment relationship, as well as the challenges posed by omnipresent surveillance and algorithmic management systems.

However, it is important to note at the outset that adopting independent employee data protection law is not a panacea for all the challenges in the workplace. The regulation of automated monitoring and algorithmic management technologies in the workplace falls under the purview of multiple legal domains. As the WP29 report observed:

‘data protection law does not operate in isolation from labour law and practice, and labour law and practice does not operate in isolation from data protection law. This interaction is necessary and valuable and should assist the development of solutions that properly protect workers’ interests.’

Therefore, the relevant legal domains including data protection law, non-discrimination law and collective rights should be combined, complement each other and utilised to address the challenges. Having said that, data protection law is uniquely placed to tackle many of the harms posed by advanced automated monitoring and algorithmic management. This is because the processing of large quantities of personal data underpins most automated monitoring and algorithmic management systems. In fact, data protection law has been the area of law that is most engaged with some of the serious harms posed by algorithmic management. For example, the GDPR has been strategically used by platform workers and their representatives to challenge some of the harmful practices of algorithmic management. In this regard, an emerging body of case law on algorithmic management in Europe shows that all the decisions by national courts and DPAs focus almost exclusively on the provisions of the GDPR or national data protection laws. This development suggests that a properly designed and adequately enforced employee data protection law could make a significant contribution to addressing the novel challenges of advanced technologies in the workplace.

A. Salient Features of the Proposed Legislation

Policymakers should consider two main issues when designing employee data protection legislation: consistency with the GDPR and the normative source of the proposed legislation.

First, for any Member State wishing to introduce employment-specific data protection legislation, taking Article 88 of the GDPR seriously should be the starting point. In other words, the interplay between the GDPR and any new employee data protection legislation should be clarified from the outset. It can be inferred from EU law and the drafting process of the GDPR that the objective of Article 88 is to allow Member States to apply or introduce specific laws

90 The decision by the Labor division of the Italian Bologna Court on the Deliveroo case is an exception, which focuses on non-discrimination law. For a comprehensive analysis of algorithmic management case law, see Christina Hießl, ‘Jurisprudence of National Courts in Europe on Algorithmic Management at the Workplace’ (European Centre of Expertise in the field of labour law, employment and labour market policies (ECE) 2023); Barros Vale and Zanfir-Fortuna (n 75).
that are ‘more favourable to workers’.\textsuperscript{91} This means that Article 88 of the GDPR is neither an exemption nor a derogation. National rules adopted pursuant to this facultative clause should particularise, complement, and strengthen the general protections of the GDPR, not water them down or deviate from them. National legislation should either stick to the minimum requirements of the GDPR or provide stricter and more protective provisions.

What does this mean in practice? The CJEU’s recent judgment Case C-34/21 provides some useful guidance on how Member States can adopt employee data protection legislation pursuant to and in compliance with Article 88 GDPR. National legislation must:\textsuperscript{92}

\begin{enumerate}
\item \textit{be consistent with the overall objectives of the GDPR.} One of the objectives of Article 88, read in light of Article 1(2) and Recital 10 GDPR, is to ensure a high level of protection of the fundamental rights and freedoms of employees with respect to the processing of their personal data. The CJEU also held that ‘when the Member States exercise the option granted to them by the opening clause of the GDPR, they must use their discretion under the conditions and within the limits laid down by the provisions of that regulation and must therefore legislate in such a way as not to undermine the content and objectives of that regulation’.\textsuperscript{93} National rules should also be consistent with the harmonisation objective of the GDPR. In this regard, the CJEU maintained that ‘lack of harmonisation may be accepted only where the differences that remain are accompanied by specific and suitable safeguards intended to protect employees’ rights and freedoms with regard to the processing of their personal data in the employment context’.\textsuperscript{94}
\item \textit{have normative content specific to the area regulated which is different from the general rules of the GDPR.} The national rules in Germany failed to qualify as ‘more specific rules’ because they simply reiterate the general requirements of the GDPR. This problem is also evident in the national laws of several other Member states. The CJEU’s decision is clear in that Member States intending to adopt ‘more specific rules’ under Article 88 should not merely repeat already existing conditions and principles of the GDPR or merely refer to those conditions and principles.\textsuperscript{95}
\item \textit{flesh out the list of specific measures set out in Article 88(2) GDPR.} In order to be classified as a ‘more specific rule’ within the meaning of Article 88(1) of the GDPR, the legislation must satisfy the conditions laid down in paragraph 2 of that Article’.\textsuperscript{96} Specifically, national rules must include suitable and specific measures to safeguard the human dignity, legitimate interests and fundamental rights of employees. This means that generally worded clauses that do not concretise and fully reflect the mandatory measures of Article 88(2) are incompatible with the GDPR.
\end{enumerate}

Second, the normative content of the proposed employee data protection legislation can be drawn from EU and national laws that are in place or in the making as well as the emerging

\textsuperscript{91} For instance, the Committee on Employment and Social Affairs also reflected this objective in its Opinion leading up to the adoption of the GDPR: ‘The right of Member States, or the social partners via collective agreements, to provide employees with more favourable protection provisions in respect of the processing of personal data in the employment context shall remain unaffected. See COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).12. This is also consistent with Article 153(4) TFEU.

\textsuperscript{92} This builds on a previous Case Note by the author. See Halefom Abraha, ‘C-34/21 - Hauptpersonalrat der Lehrerinnen: Article 88 GDPR and the Interplay between EU and Member State Employee Data Protection Rules’ Modern Law Review (forthcoming).

\textsuperscript{93} CJEU, C-34/21 (n 4) para [59], [79].

\textsuperscript{94} ibid [73].

\textsuperscript{95} ibid [74].
body of case law and policy research. In the context of algorithmic management, for instance, the Platform Work Directive and the Spanish Riders Law could well inform the substance of the proposed employee data protection rules. The emerging body of case law on algorithmic management in the workplace should also serve as an important normative source. In the past few years, several national courts and Data Protection Authorities have been called upon and intervened to resolve complex automated monitoring and algorithmic management issues. These bodies have tested the significance—or the lack thereof—of the GDPR in addressing the novel privacy and data protection harms posed by new technologies in the workplace. Although the body of case law on algorithmic management is at a nascent stage, important norms and guidelines have started to emerge. New employee data protection legislation should codify these norms and guidelines. The existing body of policy research could also play a role in articulating and identifying key regulatory issues and framing appropriate measures. Policymakers should make use of these policy proposals to develop comprehensive employee data protection legislation.

B. Normative Content of the Proposed Legislation

Without prejudice to national peculiarities and regulatory priorities, Member States that intend to introduce independent employee data protection legislation should take at least the following substantive measures as a starting point.

(i) Clarifying personal and material scope

**Personal scope:** There is a legislative trend of treating workers differently based on their legal status or the type of platform they work through. For instance, the proposed Platform Work Directive excludes traditional employees from its personal scope, which creates ‘an inconsistent regulatory environment that places workers in legal uncertainty’. New employee data protection legislation should avoid this approach. Protecting human dignity, legitimate interests and fundamental rights of workers should not depend on the legal nature of the employment relationship that binds them with the employer. From a data protection point of view, any differential treatment of workers based on their employment status would contradict the general objectives of the GDPR by creating different levels of protection. The proposed employee data protection legislation should avoid and prevent such differential treatment by rendering employment status (or the lack thereof) irrelevant. Therefore, unless explicitly stated otherwise (such as in the case of rights that exclusively apply to trade unions) and without prejudice to national peculiarities, the proposed legislation should apply to all types of workers irrespective of their employment status or the type of digital platforms they work through.

**Material scope:** The first paragraph of Article 88 GDPR provides useful guidance to determine the purposes of employee data processing which may be the subject of more specific rules adopted by the Member States. The reference to ‘processing in the context of employment’ indicates that the material scope of specific national rules should not be restricted

---

96 For a comprehensive analysis of algorithmic management case law, see Hießl (n 90); Barros Vale and Zanfir-Fortuna (n 75).

97 This section builds on previous policy research by the same authors. See Adams-Prassl and others (n 19); M Six Silberman and others, ‘REGULATING DATA-DRIVEN MANAGEMENT IN A FISSURED WORLD OF WORK’ ILR Review [forthcoming]; Halefom Abraha, ‘Regulating Algorithmic Employment Decisions through Data Protection Law’ (2023) 14 European Labour Law Journal 172.

only to data processing required solely within the contractual employment relationship. According to the case law of the CJEU, Article 88(1) relates ‘to a very large number of processing operations in connection with an employment relationship, so as to cover all the purposes for which the processing of personal data may be carried out in the context of an employment relationship’. The provision then sets out a non-exhaustive list of data processing purposes that can be addressed under specific national rules. Article 88(1) also recognises that workers have specific rights to dignity and privacy that cannot be addressed by the general rules of the GDPR. This provision requires Member States to give ‘particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the workplace.’ Therefore, subject to national peculiarities and priorities, the material scope of the proposed legislation could be derived from Article 88 GDPR.

(ii) Clarify the role of consent as a legal basis

The proposed employee data protection legislation must clarify and concretise the requirements for consent as a valid legal basis. There are legal and practical reasons why Member States should do this. On a practical level, it has long been recognised by regulatory authorities, policymakers, practitioners, and academic researchers that consent is generally an inappropriate legal basis in the employment context. The deployment of opaque and sophisticated monitoring and algorithmic management systems further undermines the validity of consent as workers are not in a position to freely give, refuse or withdraw consent.

The GDPR recognises this problem and allows Member States to provide tailored rules. According to Recital 155 (read together with Article 88) of the GDPR, Member States ‘may provide for specific rules ... for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee’. The GDPR further specifies that Member States can prohibit consent altogether if the processing involves ‘special categories’ of employee data.

New employee data protection legislation must address this legal uncertainty. Specifically, the legislation must clarify the conditions under which consent is a permissible legal basis, and identify the contexts, purposes, practices, and processing activities in which consent is inadmissible. For instance, employee data processing based on explicit consent could be permissible when the processing is associated with a legal or economic advantage for the worker. On the other hand, the legislation should explicitly prohibit consent as a legal basis for the deployment of algorithmic management systems in the workplace.

(iii) Balancing the rights and interests of employees and employers

99 CJEU, C-34/21 (n 4)63.
100 These data processing activities include, but not limited to (i) 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 employers’ or customers’ property; (ii) the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment; and (iii) the termination of the employment relationship.
101 WP 249; EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1; Kate Crawford Ifeoma Ajunwa, ‘Limitless Worker Surveillance’ <https://lawcat.berkeley.edu/record/1127979> accessed 9 February 2022; Adams-Prassl and others (n 19); Abraha, ‘A Pragmatic Compromise?’ (n 1).
102 Art. 9(2)a, GDPR.
103 ‘Interdisciplinary Council on Employee Data Protection’ (n 55).
As highlighted at the outset, the core of regulating employee monitoring and algorithmic management lies in striking a fair balance between employers’ legitimate interests and workers’ specific rights to dignity, privacy, and other fundamental rights. The question of proportionality arises specifically when employee data processing goes beyond what is strictly required within the contractual employment relationship. Any processing of employee data that is not intrinsically connected and strictly necessary for the performance of the contract must be carried out after a balancing of interests. The increasing digitalisation of the workplace makes the challenge of balancing these mutually legitimate but competing interests even more important. Unfortunately, neither the GDPR nor exiting Member State laws offer clear frameworks for conducting such a balancing exercise.

Employers are expected to conduct this balancing exercise, irrespective of the type of data practice, technology used, or the legal basis for processing. However, it should not be solely the responsibility of employers to weigh these interests. While it is not feasible for legislatures to address every possible data processing activity in the employment context, they can establish clear principles and requirements to guide employers. As the German Advisory Council on Employee Data Protection aptly pointed out, there must be binding and reliable rules enabling employers and workers to assess, with legal certainty, which decisions and measures are permissible, and which are not. In other words, new employee data protection legislation should specify the criteria and requirements for the proportionality test. It should also delineate the contexts, purposes, practices, and processing activities that are off-limits, including the continuous or permanent monitoring of workers’ behaviour. Lawmakers should also consider the circumstances and processing operations in which ‘legitimate interest’ cannot be invoked as a valid legal ground.

The principles and requirements for a proportionality test can be drawn from existing regulatory instruments, other provisions of the GDPR itself, and case law. For instance, the WP29’s Opinion 2/2017 provides ‘guidelines for the legitimate use of new technology in a number of specific situations, detailing suitable and specific measures to safeguard the human dignity, legitimate interest and fundamental rights of employees.’ The Opinion establishes a set of principles and offers a framework for proportionality assessments in several scenarios. Similar proportionality requirements and principles can be gleaned from the jurisprudence of the ECtHR. In its landmark privacy ruling in Bărbulescu v Romania, the Court outlined a list of criteria that employee monitoring must meet in order to be proportionate. These criteria include prior notification of the monitoring, extent, intensity and circumstances of the monitoring, justification of the monitoring, the necessity of methods and measures deployed, consequences for the employee, and the existence of adequate safeguards. New employee data protection legislation should codify these norms and guidelines, and to the extent possible, establish frameworks and methods for determining the ‘adequacy’ of safeguards.

(iv) Establish clear rules for algorithmic management

Algorithmic management systems have become commonplace across the economic spectrum, including in conventional employment settings, and are used by companies of all categories. While algorithmic management deserves separate regulation in its own right, the data protection requirements for the use of such technology in the employment context must be included in new employee data protection legislation. In doing so, Member States can draw the

104 ibid.
105 For details on this, see Adams-Prassl and others (n 19), Policy options 1-2.
106 Article 29 Working Party Opinion 2/2017 on data processing at work (WP 249) 8 June 2017 9 [emphasis added].
107 ECtHR, Bărbulescu v Romania, Appl No 61496/08, Para.121.
substantive content of the rules on algorithmic management from multiple sources including the proposed Platform Work Directive, existing national legislation such as the Spanish Riders Law, and other policy initiatives in Europe and beyond.\(^{108}\)

Specifically, taking the algorithmic management provisions of the Commission’s proposed Platform Work Directive as a blueprint would be a good start for Member State rules for algorithmic management. The Directive provides for more specific rules, in the context of platform work, to ensure the protection of workers’ personal data within the meaning of Article 88 GDPR. Among other protections, the Directive establishes collective rights, imposes tailored requirements for transparency and restricts the monitoring of workers. The scope of the Directive is limited only to platform work for constitutional reasons. However, the requirement to transpose the Directive into national legislation, in conjunction with Article 88 GDPR, creates an opportunity for the Member States to make it applicable to all workers subject to automated monitoring and decision-making systems, not just platform workers. The Platform Work Directive particularises the Article 22 GDPR protections and clarifies the transparency requirements for automated decision-making systems, creating legal certainty for both employers and workers. For instance, the Directive:

- Particularises the algorithmic transparency requirements stipulated under Articles 13(2)(f), 14(2)(g) and 15(1)(h) of the GDPR and expands the protection to cover both ‘solely’ automated and semi-automated decisions.\(^{109}\)
- Establishes a collective right to information by requiring employers to make algorithmic management systems intelligible to workers, their representatives and labour authorities.\(^{110}\)
- Prohibits the processing of personal data ‘not intrinsically connected to and strictly necessary for the performance of the contract’ and bans the processing of any personal data ‘on the emotional or psychological state’ of platform workers under all circumstances.\(^{111}\)
- Imposes system-level impact assessment requirements and establishes explicit rights to obtain an explanation and/or review of significant decisions in individual cases.\(^{112}\)
- Excludes consent as a legal basis to justify algorithmic management.

These rights and protections can be further specified and concretised in new employee data protection legislation.\(^{113}\) The Spanish Riders Law is another piece of legislation from which other Member States can draw helpful lessons.\(^{114}\) This law is the result of a tripartite collective bargaining agreement reached between trade unions, employer organisations, and the Spanish government. Although limited to the platform economy, the Riders’ Law establishes important data rights in algorithmic management, at both the individual and collective levels.

(v) Clarify the role of collective agreements in regulating employee data processing

\(^{108}\) Adams-Prassl and others (n 19). See also California Bill AB-1651 Workplace Technology Accountability Act 2022.


\(^{110}\) ibid Art. 6(4) ibid.

\(^{111}\) ibid art 6(5).

\(^{112}\) ibid art 8.

\(^{113}\) For detailed policy options, see Adams-Prassl and others (n 19).

\(^{114}\) Royal Decree-Law 9/2021.
The GDPR allows Member States to regulate the processing of employee data through collective agreements adopted pursuant to Article 88. However, how collective agreements interact with the GDPR requirements is not clear. As highlighted above, the CJEU is set to determine whether collective agreements alone can be considered sufficient as legal bases, or if other requirements of the GDPR must also be observed. New employee data protection legislation should clarify the extent to which collective agreements can be used as legal bases. Most importantly, Member States should adhere to the requirements that the CJEU formulates in the upcoming preliminary ruling.\footnote{Case C-65/23 Summary of the request for a preliminary ruling.}

(vi) Establish collective rights for employees

The GDPR has long been criticised for ignoring the collective rights and interests of workers inherent to the employment relationship such as the role of workers’ representatives, information and consultation of workers and the role of labour inspectorates in enforcing these rights. Furthermore, new automated monitoring and algorithmic management technologies exacerbate existing collective risks in the workplace and create new ones.\footnote{Adams-Prassl and others (n 19).} The individual rights and protections provided under the GDPR and Member State laws are crucial, but they are not sufficient to protect workers from the risks and harms posed by these technologies at the collective level. The proposed employee data protection legislation must address this issue by establishing new collective data rights and expanding the collective rights and protections provided by national laws and practices, such as co-determination rights. As pointed out by the European Commission, ‘the scope, method of exercising and content of collective rights vary from one Member State to another.’\footnote{European Commission (n 29).} Therefore, taking into account national peculiarities and practices, new employee data protection legislation must include at least the following collective rights for workers: (a) the right to organise; (b) the right to information and consultation; (c) the right to notification; (d) collective rights of data access; (e) the right to negotiate prior to the adoption of automated monitoring and decision-making technologies; (f) the right to participate in the decision-making process likely to result in significant changes in work organisation, working conditions or in contractual relations; and (g) the right to participate in data protection and algorithmic management impact assessments.

(vii) Enforcement and institutional considerations

The GDPR has an enforcement problem\footnote{The enforcement challenges of the GDPR are particularly true in transnational cases. For details on this and recent initiatives to tackle the problem, see ‘5 Years: GDPR’s Crisis Point’ (Irish Council for Civil Liberties 2023); Giulia Gentile and Orla Lynskey, ‘DEFICIENT BY DESIGN? THE TRANSNATIONAL ENFORCEMENT OF THE GDPR’ (2022) 71 International and Comparative Law Quarterly 799; European Commission, ‘Further Specifying Procedural Rules Relating to the Enforcement of the General Data Protection Regulation’ (European Commission, 24 March 2023) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en> accessed 14 September 2023.} especially in the employment context where data protection authorities often lack the resources, expertise, legitimacy, and interest to enforce workplace data protection rules effectively.\footnote{Abraha, ‘A Pragmatic Compromise?’ (n 1).} This is particularly the case in the context of automated monitoring and decision-making, which raise issues of data protection law as well as labour and social protection law.\footnote{Platform Work Directive Rec.48.} To improve effective enforcement in this context,
proposed employee legislation must take into account the following enforcement and institutional considerations.

- Establish collaborative enforcement mechanisms between different regulatory bodies. The proposed Platform Work Directive envisions a collaborative regulatory approach by allocating responsibilities between DPAs and labour authorities and requiring them to exchange relevant information relating to their respective regulatory functions.\(^\text{121}\)
- Legally mandate trade unions and workers’ representatives to participate in the enforcement of workplace data protection rules, as pointed out by the German Advisory Council on Employee Data Protection.\(^\text{122}\) This would bolster the legal position of trade unions and works councils for enforcement purposes.
- This approach should be further strengthened and expanded beyond platform work.
- Address the enforcement challenges faced by DPAs by enhancing their resources, expertise, staffing, and capacity.
- Increase the independence of data protection officers.\(^\text{123}\)

Conclusion

The increasing deployment of automated monitoring and algorithmic management technologies in the workplace gives rise to new regulatory challenges and poses significant risks to workers’ fundamental rights. The GDPR does not adequately address these challenges, as it was not intended to do so. Instead, the EU legislature leaves the regulation of employee data processing to Member States. Unfortunately, existing Member State laws are inadequate, as many fail to meet Article 88 GDPR requirements. The CJEU has established new criteria on how Member States can create separate employee data protection laws in compliance with this opening clause. Member States should take advantage of the opportunity provided under Article 88. In doing so, they must adhere to the CJEU requirements or risk the laws being invalidated later. They should also address the following main substantive issues: (a) circumstances and conditions under which consent can or cannot be used as a legal basis; (b) a framework for balancing the rights and interests of employees and employers; (c) specific rights and protections against harms arising from algorithmic management; (d) requirements for employee data processing based on collective agreements; (e) collective rights for workers; and (f) enforcement and institutional considerations.

The assessment offered by the German Data Protection Conference in April 2022\(^\text{124}\) appears increasingly irrefutable: after almost 25 years of legislative inaction, the time for enacting employee data protection law is, ‘now’.

***

\(^{121}\) Art. 19, Platform Work Directive.
\(^{122}\) 'Interdisciplinary Council on Employee Data Protection’ (n 55).
\(^{123}\) ibid.
\(^{124}\) Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2022.