NO DIGITALISATION WITHOUT REPRESENTATION

AN ANALYSIS OF POLICIES TO EMPOWER LABOUR IN THE DIGITAL WORKPLACE

Justin Nogarede

FRIEDRICH EBERT STIFTUNG

Fondation Jean Jaurès

FUNDACIÓN PABLO IGLESIAS

FONDAZIONE Pietro Nenni

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

A lack of worker influence over digitalisation

Power in the workplace is increasingly embedded in – and exercised through – the way data is collected and then used via algorithmic systems. This trend has received a boost during the Covid-19 pandemic. While this shift can – in theory – support the quality of work, at present it seems to mainly facilitate expanding surveillance and control of the workforce. To ensure a digital transition that is socially sustainable, workers and their representatives need to help shape the digital infrastructure that determines how they carry out their work. The early involvement of labour in the design and procurement of digital productivity tools will incentivise the producers of such systems to design them with workers' wellbeing in mind.

Data protection rules: unexplored potential

The General Data Protection Regulation (GDPR) is crucial for labour to gain more of a say in the digitisation of the workplace, as personal data is fundamental for many algorithmic systems that are used to monitor and direct the workforce or organise production. However, the potential of data protection rights is unrealised due to a lack of enforcement, awareness, and collective action. Data protection authorities (DPAs) need more funds to carry out systematic enforcement and guidance activities. Trade unions and works councils should become more active and invest in the capacity to help workers exercise their rights such as those to information about data collected and how this is done. There is also a strong case for involving labour in data protection impact assessments and testing the scope of provisions on profiling and automated decision-making. Finally, works councils and unions should seek as far as possible to represent collectively individual rights under the GDPR.

From data protection to data governance: collective approaches

The GDPR does not fully address the collective dimension of data processing and the risks that stem from that. Therefore, existing information, participation and co-determination rights for workers are an important additional avenue for labour to influence the deployment of digital tools at the workplace. However, the legal frameworks for labour involvement are weak in large parts of Europe and often absent in small firms. In addition, unions and works councils often lack the capacity to effectively assess or check software, let alone help shape it. At EU level, social partners have not yet effectively responded to these challenges.

To solve the collective challenges of the digitalisation of the economy, the European Commission has proposed several relevant laws for workers. Whereas the proposed Data Governance Act may facilitate responsible data-pooling, the draft law for systems of artificial intelligence (the AI Act) requires improvement. It lacks appropriate institutional structures for enforcement and opportunities for individuals to avail themselves of any rights. In addition, there are no provisions for the direct participation of workers representatives in decisions to bring AI into the workplace. In fact, it may weaken the role of organised labour in this domain.

Although the GDPR, collective rights, and new EU laws are important, they alone will not enable labour to influence the design of workplace software. Workers' involvement in the deployment of workplace technology is often late, defensively oriented, and not optimally informed, whereas co-shaping software requires pro-active and early interventions, as well as expertise. This will require new pan-European institutions and collaborations between organised labour, academia, civil society and authorities.

INTRODUCTION

INTRODUCTION

In 1974, US labour scholar Harry Braverman noted that the computer revolution was leading to the deskilling of workers and the increasing monitoring of labour and control over the workforce. Since the outbreak of the coronavirus pandemic, all signs point towards a further acceleration of this dynamic.

However, a digital future driven by Taylorist dreams of workers reduced to breathing robots is far from inevitable. Before the project was cut short by a military coup, Chile's President Allende launched Cybersyn, a national plan for algorithmic management avant la lettre, that married technology with a central role for autonomous workers. It provides evidence of the contingency of technological development and the central role of social relations. A more familiar example is Germany's system of information, participation, and co-determination rights for workers. It shows that under the right social conditions, the deployment of new technology can allow both workers and firms to thrive.[1]

The European Commission has committed itself to the notion that the digital transition should be 'human-centric'. However, a human- or worker-centric technological transition cannot be decreed from above: for the workplace, it requires that workers understand and are involved in decisions about new technology that affects their work. As US legal professor Frank Pasquale points out, algorithmic systems can be used to complement and augment human labour.[2] To progress along such a path, the voice of workers, and the role of trade unions, will be crucial.

After a short overview of current trends and potential risks surrounding data-driven algorithmic systems, this paper analyses different policy areas where EU and national institutions, trade unions and civil society organisations can act to empower workers. After looking at the potential and limitations of the General Data Protection Regulation, the paper explores the role of collective information, participation, and co-determination rights of organised labour. Finally, the potential impact of future EU laws on the digital economy are analysed, as well as what can be done to ensure workers' influence over the design of software systems for the workplace. The paper concludes with a set of policy recommendations.

---

1   S. Holmberg, 'Fighting Short-Termism with Worker Power', Roosevelt Institute (17 October 2017).
2   F. Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Cambridge, MA: Belknap Press, 2020).

No digitalisation without representation

ALGORITHMS IN THE WORKPLACE: TRENDS, RISKS, OPPORTUNITIES

ALGORITHMS IN THE WORKPLACE: TRENDS, RISKS, OPPORTUNITIES

1. Trending towards Taylorism on steroids?

The workplace is being digitalised, with an increasing collection of data and use of algorithms to manage workers, or to study them with the aim of replacing their work.[3] This trend is accelerating in the wake of the coronavirus pandemic, as employers are combining the increase in teleworking with new digital monitoring and performance-measurement tools. For instance, according to software comparison website Capterra, the demand from Dutch firms for employee-monitoring software rose by 58 percent in the first quarter of 2021, compared to 2020.[4] A recent study among senior managers at UK firms found that 20 percent installed software to monitor employees working remotely, or were planning on doing so.[5]

Figure 1: Use of data analytics for process improvement and/or monitoring employee performance, EU 27 and the UK (%)

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

Legend:
- Used for process improvement only
- Used for employee monitoring only
- Used for both process improvement and employee monitoring

---
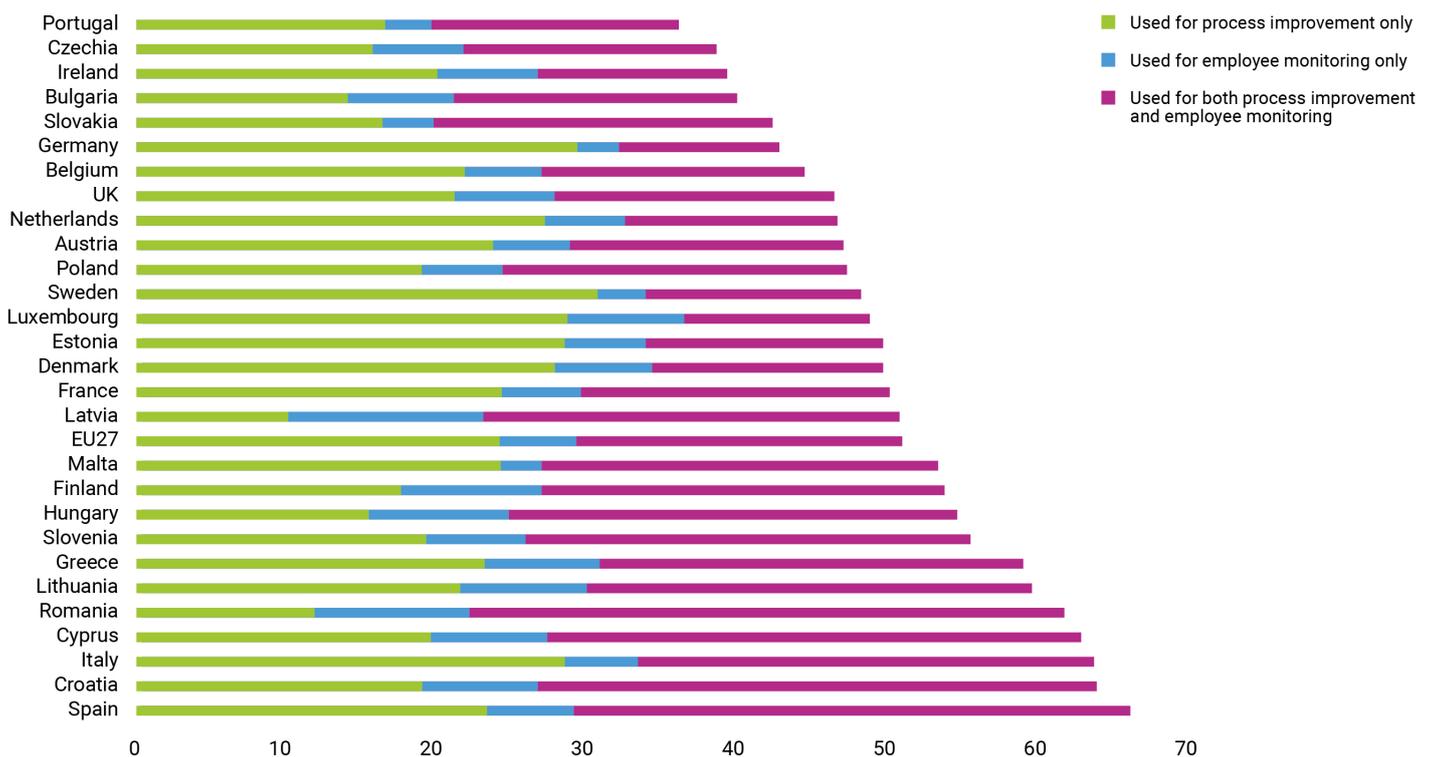
3   P. V. Moore, M. Upchurch and X. Wittaker (eds), *Humans and Machines at War: Monitoring, Surveillance and Automation in Contemporary Capitalism* (London: Palgrave Macmillan, 2018).

4   NOS, '"Gluurappartuur" in trek door thuiswerken, vakbond bezorgd', at: https://nos.nl/artikel/2375956-gluurapparatuur-in-trek-door-thuiswerken-vakbonden-bezorgd

5   Skillcast (2020), 'Remote-working Compliance YouGov Survey', 25 November, at: https://www.skillcast.com/blog/remote-working-compliance-survey-key-findings

No digitalisation without representation

Until recently, the use of workers' data for algorithmic systems in human resources, often referred to as 'people analytics' or 'algorithmic management', was considered a marginal phenomenon in Europe, limited to the platform or gig economy. However, there is evidence that **digital management tools, from online logging of hours to the performance assessment of workers, are spreading across the workforce** and are no longer confined to the gig economy.[6] In addition, the range of functions in which digital tools are being used is expanding and can cover all areas of work, from hiring to firing and everything in between (see Infobox 1).[7]

Employers' recourse to digital surveillance and algorithmic management techniques is not surprising. Firms have long tried to increase the monitoring and control of workers for the sake of higher output and lower cost. In this light, the introduction of algorithmic systems in the workplace looks like the continuation of the scientific management of the 1900s, but with different means.[8]

However, those different means matter. Providers of human resource and enterprise software offer surveillance and control opportunities that are much more intense and granular than before, such as constant logging of keystrokes and browser use, the taking of regular screenshots, and the monitoring of social media, emails and calls. In addition, sensors are becoming increasingly popular in the workplace, from wearable tracking devices and facial recognition software to systems that can track eye movements. Finally, in the interest of health and fitness, workers also partake in self-monitoring via mobile phone apps, the results of which can be shared and combined with other data sources.[9] As in particular a large study from Cracked Labs in Austria and Germany shows, such software and algorithmic systems are also offered – and used – in the EU.[10]

BOX 1: Managerial functions being automated

- Recruiting candidates

- Scheduling and allocating work

- Monitoring employees

- Evaluating worker performance

- Setting remuneration levels

- Selecting employees for promotion or other opportunities

- Triggering dismissal or disciplinary procedures

---

6   U. Huws, N. Spencer and M. Coates, 'The Platformisation of Work in Europe. Highlights from Research in 13 European Countries', FEPS, UNI Europa and the University of Hertfordshire, 2019; J. Berg, 'Protecting Workers in the Digital Age: Technology, Outsourcing and the Growing Precariousness of Work', SSRN (2019), at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413740
7   J. Adams-Prassl, 'What if your Boss was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work', *Comparative Labor Law & Policy Journal* 41(1) (2019).
8   L. Nurski, 'Algorithmic Management is the Past, Not the Future of Work', blog post 6 May 2021, Bruegel, at: https://www.bruegel.org/2021/05/algorithmic-management-is-the-past-not-the-future-of-work/
9   J. Bronowicka et al, *'Game that you Can't Win'? Workplace Surveillance in Germany and Poland* (Frankfurt (Oder): European University Viadrina, 2020), 7; A. Aloisi and E. Gramano, 'Artificial Intelligence is Watching you at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context', *Automation, Artificial Intelligence & Labor Law* 41(1) (2019).
10   Cracked Labs, 'Digital Überwachung und Kontrolle am Arbeitsplatz. Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management?' (September 2021).

Moreover, as historians of technology have pointed out, it is not simply the case that developers focus on whatever technology is most efficient or productive, and then build it. What gets developed is just as much a result of existing social (hierarchical) relations at the workplace.[12] For instance, whereas increased productivity is indeed an incentive for employers to deploy technology, so is the expansion of managerial power over the workforce, to reduce labour costs. As US law professor Brishen Rogers notes, the increase of productivity should be welcomed as it generally leads to higher labour standards, but the increase of managerial power often leads to the opposite result.[13]

For instance, in the UK of the Industrial Revolution, manufacturers understood the advantages of inventions that could help "to bypass artisan practices and controls and so sap resistance to change".'[14] Technology was designed for employers who wanted to hire children instead of adults, because children were cheaper and easier to control. The fine-grained surveillance possibilities of workplace software, as well as a decline in the labour share of the economy,[15] point to similar dynamics in today's computer revolution. For instance, **according to a large study on the EU 'people analytics' market, 'the functionality of software is often oriented to what is technically feasible, which often leaves room for deep incursions into the rights of workers**. Often, problematic functions are activated by default, and firms must deactivate those to use the system in a manner that corresponds with the law.'[16]

---

11   The definition is taken from R. Richardson, 'Defining and Demystifying Automated Decision Systems', *Maryland Law Review* 81 (forthcoming 2022).

12   L. Winner, 'Do Artifacts Have Politics?', *Daedalus* 121 (1980).

13   B. Rogers, 'The Law and Political Economy of Workplace Technological Change', *Harvard Civil Rights-Civil Liberties Law Review* 55 (2021). Of course, whether or not increased productivity translates into better working conditions depends on labour laws and the bargaining power of labour.

14   J. Humphries, 'The lure of aggregates and the pitfalls of the patriarchal perspective: a critique of the high wage economy interpretation of the British industrial revolution', *Economic History Review* 66 (3) (2013), 710.

15   C. B. Frey, *The Technology Trap: Capital, Labor, and Power in the Age of Automation* (Princeton: Princeton University Press, 2019).

16   Cracked Labs, 75.

> **BOX 3: Technology does not equal efficiency**
>
> In his article 'Do artifacts have politics?', Langdon Winner gives an instructive example of increased managerial control as a motivator for automation. In the 1880s, US manufacturer Cyrus McCormick spent 500,000 USD to add pneumatic moulding machines to his factory. The machines, however, were less efficient than the workers: they produced inferior castings at higher cost. Why, then, did he buy them? The machines made skilled workers superfluous, and these were exactly the workers who had unionised and with whom Cyrus McCormick was in conflict.[17] Today, one could think of Amazon's attempts to bust unions while using technology.

> **BOX 4: Call-centre panopticon**
>
> In 2021, the France-based call-centre service provider Teleperformance, which employs 380,000 people, announced plans to install web cams at workers' homes, to monitor whether they are eating, looking at their phone, or leaving their desks. The web cams would be connected to an 'AI' system that randomly checks for work breaches. If one is detected, the system will automatically take a picture and send it to management for corrective action.[20]

2. More control, less responsibility: risks of algorithmic management

Data collection in the workplace poses fundamental risks to worker privacy. For instance, data may relate to intimate aspects of a person, such as biometric, genetic and affective data, and can have a bearing on workers' private lives, such as sleeping patterns.[18] In addition, the tracking of GPS data, or from wearable devices, not only reveals intimate details, but also easily blurs the boundary between a workers' private and professional life. **Ubiquitous surveillance of workers has also been shown to cause stress, anxiety and a decrease in trust at the workplace**.[19]

Beyond the immediate privacy concerns linked to the collection and storage of personal data, there are further risks linked to how that data is used, and by whom. The large collection of data, from various sources, allows managers to obtain fine-grained and continuous data on worker productivity, behaviour and personal characteristics. This can be used for algorithmic systems, from basic decision-making trees to complex machine learning systems, to automate management functions and increase control over the workforce.

For instance, employers can automatically allocate work, track the performance of individual employees and rate workers according to simplified metrics (packages delivered, orders picked, words typed, emails sent). Any deviation from the mean can be observed and brought to the attention of workers and managers alike. This may lead to workers optimising for those metrics, whilst disregarding safety rules and procedures, and undermining

17 L. Winner, 'Do Artifacts Have Politics?', *Daedalus* 1(109) (1980), 124–5.
18   Autoriteit Persoonsgegevens (Dutch Data Protection Authority), 'AP: Verwerking gezondheidsgegevens wearables door werkgevers mag niet' (8 March 2016), at: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet
19   S. Sarpong and D. Rees, 'Assessing the Effects of 'Big Brother' in a Workplace: the case of WAST', *European Management Journal* 32(2) (2014), 216–22.
20   P. Walker, 'Call Centre Staff to be Monitored via Webcam for Home-Working "Infractions"', *The Guardian*, 26 March, 2021, at: https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions

professional work standards and ethics. In the words of one group of scholars, it may create a 'data-driven, performance-oriented, and overly compliance-focused organisational culture in which there is little room for moral autonomy and integrity.'[21]

While employer control is augmented, traditional structures of responsibility and accountability become more diffuse. Via the design of rating systems, the reliance on games and various incentives, employers can nudge workers' actions in a manner that is as effective as more traditional and direct forms of control, but in a way that is much less visible. Where management is partially or fully automated, it's more difficult for workers to understand the grounds for decisions, and to contest them. This is the (in)famous black box that many automated decision-making systems represent.[22]

If something goes wrong with algorithmic systems, it may be more difficult to find the cause: was it faulty data, design flaws in the system, an application error, or the decision taken by the line manager, based on the computational output? Moreover, many of the analytics systems are built by large software firms that assert proprietary rights over the workings of the algorithm, which means both employers and employees may be prevented from scrutinising decisions made and verifying whether the system respects data protection and labour laws. This is important because many ostensibly neutral systems are simply not performing as intended and may lead to discriminatory outcomes.[23]

Finally, whereas the explicit goals of the introduction of automation and algorithmic systems in the workplace are to increase efficiency, it is well known that the deployment of technology can have multiple objectives. Next to welcome increases in productivity, employers can use technology to increase their power over the workforce, which allows them to simply drive down labour costs. This can be achieved by deskilling and homogenising work, the conscious replacement of high-skilled labour, and increasing the information asymmetry between labour and management (surveillance). There is evidence that the digitisation of the workforce is indeed driving down labour costs and conditions. From Amazon's blunt use of technology to detect and thwart efforts to unionise, to Zalando's more subtle algorithmic worker performance evaluation system, which disincentivised high ratings and attendant opportunities for promotion and pay increases.[24]

Of course, none of these risks must materialise, and the judicious use of digital technology in the workplace can have real upsides. Most broadly, people analytics software may help workers concentrate and better structure their work, thereby increasing their productivity. Software to aid decision-making can also reduce biases in the hiring, promotion and firing of employees. Wearable devices can help identify risky behaviour and stress, which can support measures to increase the safety and health of workers. Monitoring of workers can help protect them in the face of unfounded complaints from customers or management. Finally, employers can have legitimate reasons to deploy monitoring tools, for instance to prevent fraud and other illegal acts, or to protect employees from harassment.

However, the positive potential of monitoring tools and algorithmic management software can only be realised when workers' rights are respected, and when they have a say in the types of technology that are being designed and deployed, and the conditions surrounding their use. Therefore, it becomes important to find ways to help workers to 'negotiate

21   U. Leicht-Deobald et al, 'The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity', *Journal of Business Ethics* 160 (2021), 386.
22   F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (London: Harvard University Press, 2021).
23   For a list, by no means exhaustive, see: https://github.com/daviddao/awful-ai
24   See P. Staab and S. Geschke, 'Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando', Study 429, Hans Böckler Stiftung (2020).

the algorithm', as professor of labour law De Valerio has put it.[25]

25 V. De Stefano, 'Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection', *Comparative Labour Law & Policy* 41(1) (2019).

PROTECTING DATA, EMPOWERING WORKERS: THE POTENTIAL OF THE GDPR

PROTECTING DATA, EMPOWERING WORKERS: THE POTENTIAL OF THE GDPR

Since 2018, the General Data Protection Regulation provides a set of horizontal rules covering the processing of personal data, including in the workplace. This is an important regulation, because many of the algorithmic systems that are used to manage workers rely on the collection and processing of the personal data of workers. By setting out legal standards for the collection and use of workers' personal data, the GDPR offers an important tool for workers to use to shape technological developments in the workplace and rebalance the power dynamics between management and the shop floor.

The GDPR is especially potent, because it contains norms that are not limited to the protection of workers' privacy, but that cover a broader set of their fundamental rights, as well as profiling and automated decision-making. This is important, as co-determination rules over new technology in the workplace vary widely across Europe, and in some countries and workplaces it may be the best tool workers have available to them. However, before the data protection rules can play their full role, they need to be better explained and enforced, and workers' representatives can play a key role in these efforts.

3. Workers' data protection: lack of awareness, lack of enforcement

The General Data Protection Regulation has entered its fourth year of application, but its significance and potential for the protection and advancement of workers' interests is still largely untapped. Although the number of fines is slowly starting to pick up, with over 60 fines across the EU that are directly employment related,[26] evidence suggests a lack of awareness among workers of their rights, a lack of action from trade unions and a dearth in enforcement by DPAs.

First, it appears that many workers may not be aware of their privacy and data protection rights.[27] In a recent survey carried out by the Christian National Trade Union Federation in the Netherlands, 13 percent of respondents said they were monitored while working from home, which is only allowed in exceptional situations, and requires both justification and works council approval.[28] The Dutch Data Protection Authority also notes that they receive few complaints from workers, which in their view may be related to workers' lack of understanding about the extent of surveillance.[29] The hierarchical character of the employer–employee relationship might also play a role here.

Second, there is reason to believe that the problems of non-compliance and under-enforcement of data protection rules are especially striking in the workplace. Recent research in Poland and Germany notes that levels of monitoring of call centre employees at times 'could be deemed excessive'. The study also highlights that the GDPR did not

---

26   CMS, 'GDPR Enforcement Tracker', at: https://www.enforcementtracker.com. The database aims to collect all publicly available fines decisions of Data Protection Authorities. It is not complete, but gives an indication.
27   J. Bronowicka et al, 24.
28   CNV, 'Half miljoen thuiswerkers via software in de gaten gehouden', at: https://www.cnv.nl/nieuws/half-miljoen-thuiswerkers-via-software-in-de-gaten-gehouden/
29   NOS, '"Gluurappartuur" in trek door thuiswerken, vakbond bezorgd', at: https://nos.nl/artikel/2375956-gluurapparatuur-in-trek-door-thuiswerken-vakbonden-bezorgd

Figure 2: EU Data Protection Authorities' fines for employment related GDPR breaches

Country	Fines
Spain	14
Italy	13
Hungary	7
Romania	5
Cyprus	4
Greece	4
Luxembourg	4
Bulgaria	3
Finland	3
Germany	3
Czech Republic	2
Denmark	2
Netherlands	2
France	1
Latvia	1
Sweden	1
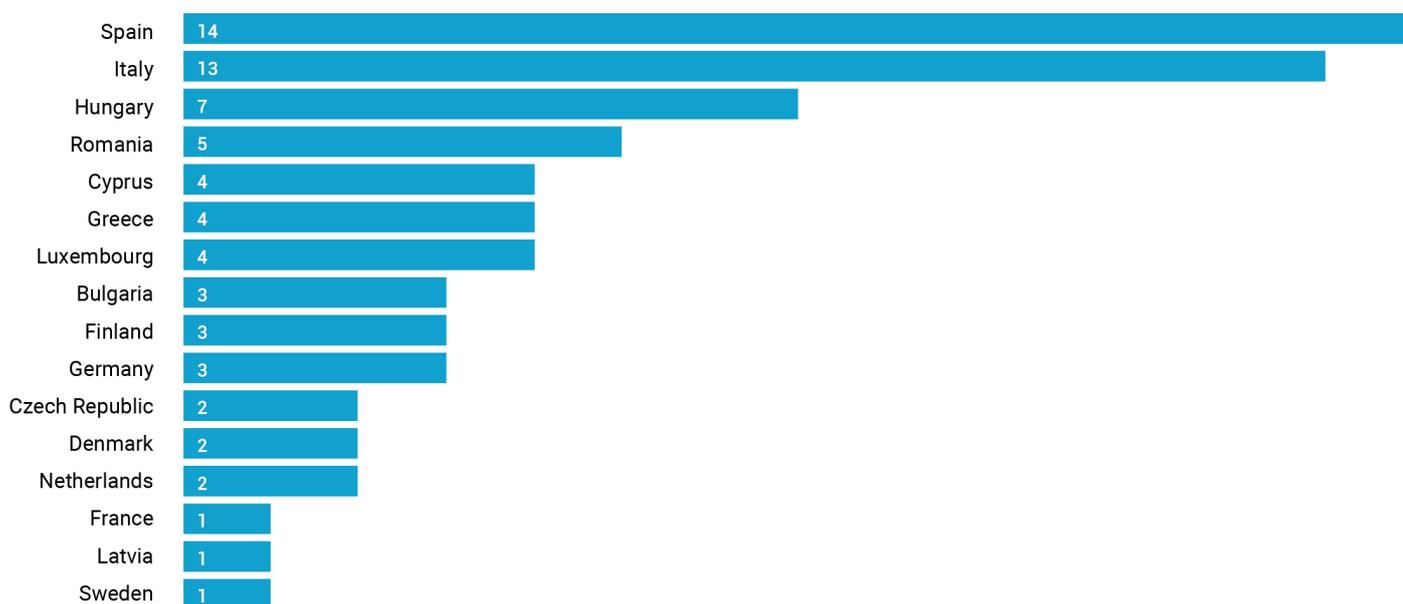
This chart is based on publicly available information gathered by CMS Law's GDPR Enforcement Tracker since the GDPR became applicable in 2018. It might not give a complete picture, as Data Protection Authorities are not obliged to publish enforcement decisions. Cases after 15 November 2021 are not included.

lead to a structural change in the level of employee monitoring, at least insofar as workers who were interviewed could tell.[30] When Prospect Union in the UK polled over 7,500 workers, **48 percent were 'not confident' or 'not confident at all' that they were informed about the data collected about them by their employers**.[31] Although this is not direct evidence of non-compliance, it does put into question whether the GDPR has been able to create a level of trust and transparency for the processing of personal data in the workplace.

This should be a reason for DPAs to pay special attention to data protection in the workplace. As the main institutions entrusted to make sure that data protection rules are respected throughout the

EU, they are obliged under Article 57 of the GDPR to investigate, proactively monitor and enforce the application of the data protection rules. In addition, any complaint they receive must be followed up, unless it is manifestly unfounded or excessive. Unfortunately, DPAs are not carrying out the legal obligations they are entrusted with.

According to reporting from the European Data Protection Board, the coordinating body of European DPAs, funding needs from many DPAs are not being met. Some authorities report underfunding of close to 100 percent.[32] In addition, there are large disparities between the different authorities' budgets. As the Irish Council for Civil Liberties recently reported, Germany's DPAs account for 32 percent of the

---

30 J. Bronowicka at al, 21, 39.
31 Prospect, 'Union Reveals that Half of Workers Don't Know What Data their Boss Collects About Them', 12 February, 2020, at: https://prospect.org.uk/news/union-reveals-that-half-of-workers-dont-know-what-data-their-boss-collects-about-them/
32 European Data Protection Board, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities', 26 February, 2019, 7, at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

entire accumulated budget of all EU DPAs. At the same time, **half of all authorities still operate on a budget of 5 million EUR or (significantly) less**.[33] This translates into long delays in the handling of complaints, as well a lack of meaningful follow-up and fines. Although the failure of DPAs to treat well-founded complaints is a dereliction of duty that can be challenged in court, complainants should not have to sue the authorities that are supposed to protect them to make good their rights.

BOX 5: DPAs and dereliction of duty

In its annual report of 2020, the Dutch Data Protection Authority admits it lacks the resources to carry out its legal oversight tasks. It notes having a backlog of 1,500 complaints, as well 8,300 tips that it cannot act upon. Most worryingly, it cannot carry out oversight of algorithmic systems that process personal data. The Dutch Authority is among the better resourced agencies within the EU.[34] This means the move to algorithmic management at work is left unsupervised in the Netherlands.

In addition, many DPAs are still reluctant to effectively use their scarce resources in a manner that maximises impact. For instance, they often fail to focus on big firms that routinely flout the rules.[35] Many DPAs are also reluctant to aggressively enforce the rules by imposing substantial fines. This is especially problematic if the number of cases they investigate is already very limited. When both the chance of getting caught and of receiving a

significant fine are in practice limited, firms have few incentives to comply.

BOX 6: The shortcomings of GDPR enforcement. A case study

Zalando's employee performance system, called Zonar, incentivised employees to continuously provide feedback about colleagues via software. This feedback was transformed into individual ratings that would determine workers' opportunities for promotion, pay increases and could have had effects on continued employment.[36]

After a year-long investigation, the Berlin Data Protection Authority concluded that the collection and storage of personal data infringed the GDPR, and that the '360-degrees performance feedback' could lead to ubiquitous surveillance pressure on workers. Nevertheless, it did not fine Zalando. Instead, it advised Zalando on how to make the software GDPR compliant.

This case exemplifies the hurdles for employees' data protection. First, the DPA acted over a year after concerns were being raised publicly about Zonar. Second, the guidance provided by the DPA was not public, and specific to Zalando, and no fines were handed down, even though non-compliance with the GDPR was observed. This means there are no broader effects from the DPA's involvement, be they pedagogic

---

33   J. Ryan and A. Toner, 'Europe's Enforcement Paralysis. ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities', Irish Council for Civil Liberties, 2021.

34   Autoriteit persoonsgegevens, 'Jaarverslag 2020' (2021), 11–12, at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf

35   J. Nogarede, 'Governing Online Gatekeepers: Taking Power Seriously', FEPS, 2021, 29–30; Noyb, 'Luxemburg's Watchdog Refuses to Show its Teeth to US Companies', 25 January, at https://noyb.eu/en/luxemburgs-watchdog-refuses-show-its-teeth-us-companies.

36   For an in-depth analysis of Zalando's Zonar software, see P. Staab and S. Geschke, 'Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando', Study 429, 2020, Hans Böckler Stiftung.

> or dissuasive. Lastly, apparently works councils (and unions represented in them), where they existed within the company, were unable to detect GDPR non-compliance.

Finally, many DPAs do not consider the workplace a priority domain for their enforcement activities. An analysis of the strategic and operational priorities of 12 European DPAs showed that only three featured employment.[37] In addition, **the European Data Protection Board does not once mention employment in its Work Programme for 2021–22**. This is disconcerting, in light of the accelerated digitisation of the workplace spurred on by the coronavirus pandemic, which should catapult workers' data protection to the top of the list.

4. For an activist trade union role

Although the GDPR explicitly applies to workers' data, the interpretation of data protection principles at the workplace is still in its infancy. Many provisions remain to be interpreted and clarified. The Article 29 Working Party (the predecessor of the European Data Protection Board) provided an interpretation in 2017,[38] but there have been repeated calls for additional guidance on privacy and data protection at work.[39] In the context of the European Commission's 2020 review of the GDPR, stakeholders also signalled a need for additional guidelines on 'the scope of data subject rights (including in the employment context)'.[40] Such guidance would push back against obvious abuses, such as cases where employers use the GDPR's data protection provisions as a pretext

to withhold information from workers and workers' representatives.[41]

According to Article 88 of the GDPR, member states may provide more specific rules, by law or collective agreements, for the processing of employees' personal data in a work context. However, most member states have not availed themselves of the opportunity to do so. Given in particular the dearth in enforcement and case law to provide authoritative interpretations of data protection principles in the workplace, this would be a very helpful step.

Nevertheless, trade unions and workers' representatives at company level do not have to wait for such clarification via specific national rules or via collective agreements. The GDPR already contains articles that can help workers to make good on specific data protection rights, and that could also offer broader protection of workers' fundamental rights in a digitised workplace full of 'people analytics'. However, it is by now clear that DPAs alone cannot effectively ensure the law is enforced in workplaces across the EU. Therefore, organised labour should increase its role in the effective implementation of the GDPR. This can also be an important springboard for an increased union role in the wider debate on the digitisation of work.

First, unions, as well as their shop floor representatives, can take part in awareness-raising and training at the workplace. They should also invest in resources to develop working relationships with the data protection officer (if present at the firm) and the competent DPA, to facilitate better enforcement of the law, not only after complaints have been raised, but also before. Unions can also take an active role in the enforcement of data

---

37   C. Kress, R. Van Eijk and G. Zanfir-Fortuna, 'New Decade, New Priorities: A Summary of Twelve European Data Protection Authorities' Strategic and Operational Plans for 2020 and Beyond', Future of Privacy Forum, 12 May 2020, at: https://fpf.org/wp-content/uploads/2020/05/FPF_DPAStrategiesReport_05122020.pdf

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

39   F. Hendrickx, E. Gramano and D. Mangan, 'Privacy, Data Protection and the Digitalisation of Work: How Industrial Relations Can Implement a New Pillar', Kluwer Regulating for Globalization Blog, 26 June 2020, at: http://regulatingforglobalization.com/2020/06/26/privacy-data-protection-and-the-digitalisation-of-work-how-industrial-relations-can-implement-a-new-pillar/

40   European Commission, SWD (2020), 115.

41   S. Stolton, 'Employers Accused of Abusing EU Data Privacy Rules to Hinder Trade Unions', Euractiv, 19 March, 2020.

protection rights. For instance, Article 80(1) of the GDPR allows non-profit organisations, including unions, to represent workers and act on their behalf when it comes to lodging complaints with DPAs, or to make good on their right to an effective judicial remedy. This can be an opportunity for trade unions to develop a presence and role in an area that is vital for workers' working conditions.

> **BOX 7: Data shop stewards**
>
> In 1971, the Iron and Metalworkers' Center in Norway hired the Norwegian Computing Center to study new digital technology that was being introduced in the workplace. It resulted in the creation of 'data shop stewards', who would study new technologies on behalf of the union and suggest changes to systems to safeguard workers' interests.[42] Since then, Norwegian labour rules allow for the creation of 'data shop stewards' in both the private and (until recently) public sectors.

Second, Article 80(2) allows member states to appoint non-profit organisations, such as trade unions, that have the legal standing to file complaints to DPAs and data controllers when it considers the rights of data subjects have been infringed. Unfortunately, many member states have not used the option to nominate unions, consumer organisations and other civil society organisations, so that they can bring such complaints.

> **BOX 8: Collective enforcement of the GDPR**
>
> French legislation implementing the GDPR allows trade unions to bring 'data class action' suits, if the processing of personal data affects the interests of the individuals that these organisations are entrusted to defend. This can be a model for other member states to follow.

5. Low-hanging fruit: key GDPR provisions for worker empowerment

5.1 Legal base for processing personal data

The GDPR only allows the processing of personal data if there is an explicit legal base. In the online economy, firms often rely on the consent of users. However, because the employer–employee relationship is hierarchical, employees cannot normally satisfy the GDPR definition of consent, which requires 'any freely given, specific, informed and unambiguous indication of the data subjects' wishes'. The Article 29 Working Group stated that 'employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances."[43] Moreover, consent needs to be a specific and informed indication of an employee's wishes. That means any default settings on devices or installed software cannot satisfy that requirement.

Alternatively, employers could justify the processing of workers' personal data as being necessary for the pursuit of a legitimate interest. This could for

---

42   D. F. Noble, 'Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools', in eds D. Preece, I. McLoughlin and P. Dawson, *Technology, Organizations and Innovation: Critical Perspectives on Business and Management. Volume 1: The early debates* (London: Routledge, 2000), 395.
43   Article 29 Working Party (2017); see also Recital 41, GDPR.

instance entail the monitoring of employees to protect employee safety, secure company assets, and manage workplace productivity. However, this should always be balanced against employees' fundamental rights: can they reasonably expect to be under surveillance? Not, German courts judged, for the secret installation of key-logging software.[44]

In any case, when employers aim to process employee data in pursuit of a legitimate interest, they must still comply with the general principles of data minimisation, proportionality and transparency. The latter point is often neglected: employers should always inform workers about the nature, scope and objectives of any processing of workers' personal data.

> ## BOX 9: Legal grounds for processing workers' data
>
> **Employers cannot normally rely on workers' consent for the introduction of surveillance. The obvious legal base is an employer's legitimate interest, which requires careful balancing against workers' fundamental rights, and must be necessary, proportionate and transparent. Hence, indiscriminate surveillance of employees is always illegal under the GDPR.[45]**

Given the rapid adoption of workplace monitoring software that process personal data, which cannot legally take place by merely relying on workers' consent, there is an opportunity for workers, and especially their representatives. They can challenge such practices and engage management in a discussion on the goals, proportionality and modalities of systems that rely on the processing of workers' personal data.

5.2 Data protection impact assessments

Following Article 35 of the GDPR, employers should carry out data protection impact assessments, before implementing digital technologies that involve the processing of personal data and which are likely to result in a high risk to rights and freedoms of employees.[46] What counts as high risk has been clarified by the Article 29 Working Party, and individual DPAs have also listed situations where such an impact assessment is required. These include 'evaluation or scoring', the involvement of vulnerable subjects – which should include employees – and systematic monitoring. Together these mean that hardly any system that monitors and/or assesses workers' performance should be exempt, especially if such systems also result in the taking of automated decisions.

---

44   Bundesarbeitsgericht, 27 July 2017, 2 AZR 681/16.
45   The other exceptions, such as the compliance with legal obligations (tax contributions), or for the performance of a contract (calculation of employee remuneration), are narrow and normally not at issue.

Table 1: Article 35 GDPR: examples of data processing requiring a DPIA according to DPAs

Country	Activity	Example
NL	Performance assessment	Systematic and extensive assessment of people, for instance the job performance of employees
IT	Remote monitoring	Processing in context of employment relationship through technological systems (video surveillance, geolocation) which allows the remote monitoring of employees' activities
FR	HR management	Establishing a profile on individuals for HR management purposes

Once the need for an impact assessment has been established, the GDPR requires that a 'data controller' (the employer) seeks the views of data subjects or their representatives, *where appropriate*. Given that the GDPR is more stringent when it comes to processing in-work relationships, it can be argued that Article 35 should be interpreted strictly as well. This implies that employers are obliged to consult employees when carrying out an impact assessment for data processing operations that will affect the latter.

The UK Information Commissioner's Office agrees that data controllers should 'seek and document the views of individuals (or their representatives), unless there is a good reason not to' (which should be documented and explained).[47] Of course, in member states such as Germany, labour laws already oblige employers to consult worker representatives for data protection impact assessments, but this is not the case in all of the EU.

By involving employees or their representatives, impact assessments can also become more relevant. Research has identified that data protection impact assessments easily risk turning into abstract compliance exercises that shield organisations from liability, rather than leading to reduced risks for data subjects (workers) and more privacy-friendly products.[48] By bringing in the views of workers, adverse impacts on their fundamental rights (not just privacy) can be better considered.

---

46   In addition, such DPIAs should be periodically reassessed, which is especially important in light of machine learning applications, the functioning of which may change over time. See Article 29 Working Party (2017) WP 248, 4 April 2017, 19, at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

47   Information Commissioner's Office, 'How Do We Do a DPIA?', at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7

48   F. Ferra, I. Wagner, E. Boiten et al, 'Challenges in Assessing Privacy Impact: Tales from the Front Lines', *Security and Privacy* 3(2) (2020).

5.3 Profiling, automated decision-making and the GDPR

When workers' personal data is used to analyse or predict their behaviour, interests and performance at work, this is referred to as profiling. Based on such profiles, algorithmic systems can also take decisions about workers, for instance on work schedules, pay and promotion. The GDPR offers rights and protections against such practices, for instance by increasing transparency, and by allowing workers to demand a human assessment instead of an automated one.

The rights afforded by the GDPR (and its predecessor) against profiling and automated decision-making have hardly been invoked and have not had much practical effect on the development of information systems. Some attribute this to the complexity of the provisions.[49] Whilst this may be true, a careful reading of the relevant provisions shows workers and their representatives can rely on the GDPR to receive information about algorithmic decisions that affect them, and to limit their use.

The main provision on automated decision-making is Article 22, which allows workers the right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects them. Although the provision speaks of a right, it is best seen as a prohibition, which suits the overall objective of the GDPR (strengthening the protection of personal data). This reading also corresponds with Recital 71, which states that 'automated decision-making, including profiling, should be allowed where expressly authorised by law, or necessary for the entering or performance of a contract, or when the data subject has given explicit consent.' In other words, in the absence of those grounds, it should be forbidden. This is also consistent with the guidelines from the Article 29 Working Party.[50]

The exception that allows automated decision-making for the performance of a contract has the condition that it is 'necessary'. In practice, this means there must be no other way of performing the contract. A reasonable interpretation would mean that decisions regarding promotions, bonuses and especially dismissals can never be taken in an automated fashion, as their scale would never be such as to make human intervention impracticable.[51] This view also aligns with the EU's broader approach to artificial intelligence, which requires humans to be in command.

---

49   L. A. Bygrave, 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making', University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2019-01, 2019, 3–4.

50   Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2017, 19.

51   A. Todolí-Signes, 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection', ETUI, 2019, 7–8.

Admittedly, some have interpreted Article 22 as applying only to fully automated systems. Such a reading would exclude all systems that provide 'decisional support', or where there is still a human in the loop, however spurious his or her role may be.[52] This would lead to absurd results as it would leave workers defenceless against some of the most automated employee performance management systems, such as Amazon's ADAPT system. This system quasi-automatically leads to people being fired after a set number of automatically generated warnings. Indeed, many legal scholars argue against such a narrow literal interpretation.[53]

Figure 3: Amazon's ADAPT performance measurement software[54]
'You are expected to meet 100% of the productivity performance expectation. Please note that if an associate receives a 2nd final or a total of 6 documented counselling write-ups in a rolling 12 months, their employment will end.'

Performance Trend. Below is a summary of your past Productivity performance

Period Start	Unit Count	Hours Worked	UPH	% to Goal	% to Curve	Exempted
May 01, 2019, 5:00:00 AM	5038	16	324	82.23	82.23	N
April 24, 2019, 5:00:00 AM	1759	5	348	87.9	87.9	Y
April 17, 2019, 5:00:00 AM	0	0	0	0	0	Y
April 10, 2019, 5:00:00 AM	1856	6	317	80.47	80.47	Y
April 03, 2019, 5:00:00 AM	4272	12	347	88.28	88.28	Y
March 27, 2019, 5:00:00 AM	0	0	0	0	0	Y

---

52   S. Wachter, B. Mittelstadt and L. Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law* 7(2) (2017).
53   M. Veale and L. Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling', *Computer Law & Security Review* 34(2) (2018); A. D. Selbst and J. Powles, 'Meaningful Information and the Right to Explanation', *International Data Privacy Law* 7(4) (2017).
54   Amazon's ADAPT performance measurement tool, assessment of employee Parker Knight, accessed at https://www.revealnews.org/wp-content/uploads/2019/11/Parker-Knight-productivity-report.pdf. See also: Will Evans, 'Ruthless Quotas at Amazon Are Maiming Employees', *The Atlantic*, 5 December (2019). https://www.theatlantic.com/technology/archive/2019/11/amazon-warehouse-reports-show-worker-injuries/602530/.

As Todolí-Signes convincingly argues, when algorithms 'take' a decision and a human operator merely *applies* it, it would still fall under the protection of Article 22. More broadly, he argues that fully automated decision-making does not exist. Algorithms do not have a will: humans are always taking the decisions, either by programming the algorithm or by applying its outcomes. As human intervention is always necessary, it cannot mean that such intervention would prevent workers relying on the defences of Article 22, because they would then never be applicable.[55] Such an interpretation also finds support from AI and computing experts.[56]

When it comes to transparency, workers have the right to know that automated decision-making (fully or partially) is playing a role in their work, the right to meaningful information about the functioning of the algorithm concerned (parameters, weighting), and the right to be informed about the consequences of the process. This flows from Articles 22(3), 13(2)(f) and 14(2)(g), in combination with the general principle of the transparency of processing.

It is true that Wachter et al deny the existence of a right to a specific explanation after the information has been collected, about why a decision has been taken.[57] However, Recital 71 recalls that profiling and automated decision-making should be 'subject to suitable safeguards, which should include *specific* information to the data subject [...], to express his or her point of view, to obtain an *explanation of the decision reached after* such assessment and to challenge the decision.' This supports the case for

the right to a specific explanation, after a decision has been taken.

Such an interpretation also aligns well with the purpose of this provision, which aims to help individuals to detect and challenge unfair and discriminatory decisions that affect them. This would hardly be possible were employers only required to provide the most generic explanations of the workings of an algorithm. This would not allow workers to understand, say, the rejection of an application or the grounds of a dismissal, and yet the explanation of automated decisions should be sufficiently comprehensible, according to the Article 29 Working Group guidelines.[58] Overall, the notion of a right to an explanation has been supported by a variety of scholars.[59]

---

55   A. Todolí-Signes, 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection', ETUI, 2019, 7–8.

56   J. Bryson, 'The Past Decade and Future of AI's Impact on Society', in *Towards a New Enlightenment? A Transcendent Decade* (Madrid, BBVA, 2018).

57   Wachter, Mittelstadt and Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 92.

58   Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2017, 25.

59   A.D. Selbst and J. Powles, 'Meaningful Information and the Right to Explanation', *International Data Privacy Law* 7(4) (2017); Lee A. Bygrave, 'Article 22', in eds C. Kuner, L. A. Bygrave and C. Docksey, *Commentary on the EU General Data Protection Regulation* (Oxford: Oxford University Press, 2019); I. Mendoza and L. A. Bygrave, 'The Right Not to be Subject to Automated Decisions Based On Profiling', in eds T. Synodinou, P. Jougleux, C. Markou and T. Prastitou, EU Internet Law: Regulation and Enforcement (Springer: 2017), 77–98.

No digitalisation without representation

BOX 12: GDPR and the right to an explanation

In a recent legal dispute between workers and ride hailing service Ola, the Amsterdam District Court found that workers were owed an explanation from the company about the logic and criteria underpinning an automated decision-making system that could issue monetary penalties to drivers. The Court also ruled those workers should be able to request a human assessment, instead of a fully automated decision. Although the ruling can still be overturned, it suggests the GDPR can offer respite to workers beyond data protection concerns, and that the GDPR may indeed contain a right to an explanation for 'fully' automated decisions.[60]

The limits the GDPR sets for personal data collection, combined with the information and consultation requirements of workers, including when analysing and using personal data for decision-making, already provide significant scope to make sure workers are heard and consulted in the implementation of digital technology in the workplace.

---

60   Rechtbank Amsterdam, Uitspraak 11-3-2021, c/13/689705.

THE DIGITISED WORKPLACE: FROM DATA PROTECTION TO DATA GOVERNANCE

THE DIGITISED WORKPLACE: FROM DATA PROTECTION TO DATA GOVERNANCE

6. When data is plural, governance should be collective

The General Data Protection Regulation mainly focuses on the protection of the rights of individuals. However, an increasing number of authors highlight that the focus on individuals is not sufficient in an era of big data, for the following conceptual, economic and practical reasons.

First, conceptually, data are rarely relevant for just one individual. When someone decides to share information about their DNA, that also implicates their blood relatives, even though they have no say in the matter. Similarly, data provided by an individual employee (emails, location data, voice recordings, performance-tracking) will often affect co-workers.

Therefore, it is not sufficient to look at data governance exclusively through the prism of the individual and vertical relation between someone whose data is processed, and the (legal) person doing the processing. As S. Viljoen explains, the production of data often concerns 'horizontal relations', where information about personal characteristics or location about one person may affect others who share similar characteristics.[61] This requires collective forms of data governance, both to manage the risks and to realise the potential of (personal) data collection and analysis.

Second, the economic drivers of data production also focus on the aggregate, not the individual. The main incentive for the collection of personal data is to establish links between individuals, and to build profiles to predict and modify the behaviour of groups of people. These techniques have been pioneered in the advertising industry (behavioural ads) but are spreading across the economy and society. Based on large troves of personal data, firms build profiles about groups of people. While profiles can include characteristics that are familiar and protected under anti-discrimination law, like age, sex and race, there are hundreds of variables that are not covered under anti-discrimination law, and which are not intuitive and therefore difficult to detect or understand by the people affected.[62]

Third, the use of data to build profiles about groups of people may not be easily relatable to the personal data on which they are built, due to the scale and use of anonymised data. This makes it difficult for affected people to rely on the GDPR.[63] In addition, although the GDPR contains a right to explanations of algorithmic decisions with important effects, there is no 'right to reasonable inferences'. People affected by algorithmic decisions have no practical means to make sure that such decisions are based on reasonable inferences.[64]

Of course, the information and power asymmetries that now characterise the digital economy are very

---

61   S. Viljoen (forthcoming), 'Democratic Data: A Relational Theory For Data Governance', *Yale Law Journal*.

62   The European Commission has tabled legal proposals to tackle some of these issues, see: 'Digital Markets Act', COM/2020/842 final and 'Digital Services Act', COM/2020/825 final.

63   A. Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection', *Computer Law & Security Review* 32 (2017), 238–55.

64   S. Wachter and B. Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review* 2 (2019), 12.

familiar, and more acute in the hierarchical relations between management and workers. To address those imbalances, European countries have since long put in place an elaborate system of collective governance, in which institutions such as trade unions and works councils ensure workers are collectively represented and receive information about and actively influence management decisions.

While we see the attempt to export such collective systems from the world of work to consumer issues in the digital economy, like the initiative for 'data unions' to bargain with the likes of Facebook,[65] it is an open question as to how effective they are in shaping the digitisation of the workplace itself. The GDPR does allow unions and workers' representatives to become involved in data protection issues. Both explicitly in Article 88 – which calls for specific data protection measures to be provided via collective agreements – and implicitly, by mentioning that individual consent is as a rule an invalid ground for the data processing of workers, as the latter's consent cannot be freely given, due to the hierarchical work relationship.

7. Collective solutions: information and co-determination rights

Labour law provisions on information and participation rights of workers, from the European level down to the individual firm, provide exactly some of the collective mechanisms that would allow workers to influence the direction of technology in a manner that data protection law currently lacks. They are the best tool available to ensure digitisation leads to increased productivity and better working conditions. That said, the level of practical protection

and influence workers have collectively varies greatly across Europe, for a few reasons.

7.1 Employee representation at the firm

First, employee representation at the firm level via works councils is highly developed in countries like Germany, where such councils must be consulted on any new technology in the workplace. But in many countries in South and Eastern Europe, works councils are less common and where they do exist, they often have few rights, limited to the receipt of information after decisions have been taken. Whereas countries like Germany, France and the Czech Republic foresee employee representation on the management board of larger firms, this is non-existent in, for instance, the Baltic countries and absent for private-sector firms in most other European countries, including Italy, Spain and Portugal.[66]

However, even in Germany, the reality is that many firms lack participation and co-determination structures. **For instance, in Germany, one of the EU countries with the most developed legal framework and praxis, in 2019 fewer than 40 percent of employees worked in a firm with a works council.**[67] Smaller firms in particular often lack structures for worker participation. This is problematic, because SMEs especially are at risk of adopting off-the-shelf people-management software without the necessary safeguards in place. This puts into question the EU's official policy goal to ensure the rapid digitisation of SMEs across Europe.[68]

---

65   See for instance the Dutch initiative to create a data union to collectively negotiate with Facebook and Google about their policies about user data, at: https://thedataunion.eu

66   See the European Trade Union Institute's database on worker participation issues across Europe, at: https://www.worker-participation.eu

67   For former West Germany, only 41 percent of employees worked in a firm with a works council (from firms with a staff of 5 or more). For former East Germany, the percentage was lower, with 36 percent of employees. See P. Ellguth, 'Ost- und Westdeutschland nähern sich bei der Reichweite der betrieblichen Mitbestimmung an', IAB-FORUM, 13 May 2020, at: https://www.iab-forum.de/ost-und-westdeutschland-naehern-sich-bei-der-reichweite-der-betrieblichen-mitbestimmung-an/

68   See European Commission, 'Digital Compass 2030' (2021), COM/2021/118 final.

In addition, decision-making power in larger firms, and in the design and functioning of technical systems, is increasingly centralised, and moves away from the shop floor. For instance, in a survey by IG Metall among works councils and shop stewards at close to 2,000 firms, **87 percent of councils said that key decisions on transformation are taken at company and group level**.[69] Companies and industries themselves are also becoming more concentrated.[70] On a technical level, the 'agile turn' and the move to cloud-based software services implies that more and more systems are regularly updated and maintained by large cloud providers.[71] These often globally operating firms protect their software with intellectual property rights and trade secrecy laws, to prevent outside scrutiny.[72]

According to a large investigation by Cracked Labs into the EU market for employee monitoring and management software, the move to rely on cloud services from third parties means that firms lose direct control over the software and hardware they use. The author notes that software functions and data processing practices are highly standardised, and that even internal IT departments have a hard time figuring out what exactly happens in the cloud.[73]

Given that, it is not surprising that labour representatives are in practice not able to effectively scrutinise (let alone co-design) all software updates, even when this is a legal requirement. For instance, in interviews with works council members of several firms in Austria, it becomes clear that a host of algorithmic processes are not effectively supervised by works councils, likely illegally.[74]

The difficulty for works councils in keeping up with developments seems to be borne out by the – admittedly limited – data and research that is available. For instance, an analysis of over 1,100 collective bargaining agreements concluded at companies in Italy between 2015 and 2018 highlights that trade unions and workers' representatives generally take a defensive approach, mainly aiming to protect workers from invasive surveillance and control mechanisms. According to the authors, only episodically "it is possible to detect first signs of a more proactive role of workers' representatives that go as far as co-determining the purposes and procedures of data processing, thus making efforts to embed datafication trends with a social and collective perspective."[75]

Furthermore, the dynamic character of AI systems requires works councils to monitor the use permanently, as learning systems might change their character during operation. Instead of simply

69   K. Schäfers and J. Schroth, 'Shaping Industry 4.0 on Workers' Terms. IG Metall's Work_Innovation Project', Trade Unions in Transformation 4.0 series, Friedrich-Ebert-Stiftung, September 2021, 11.

70   See for instance J. De Loecker and J. Eeckhout, 'Global Market Power', NBER Working Paper 24768 (2018).

71   S. Gürses and J. van Hoboken, 'Privacy After the Agile Turn', in eds Evan Selinger et al, *Cambridge Handbook of Consumer Privacy* (Cambridge: Cambridge University Press, 2018).

72   See O. Lobel, 'The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property', *Texas Law Review* 93(789) (2015), and J. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019).

73   Cracked Labs, 75–6.

74   Cracked Labs, 137–43.

75   E. Dagnino and I. Armaroli, 'A Seat at the Table: Negotiating Data Processing in the Workplace', *Comparative Labor Law & Policy Journal* (2020), 173–95.

agreeing on how an application is used, works councils must demand regular consultations with management and push for conflict-resolution agreements that allow for adjustments as the system is changing.[76]

7.2 The role of unions

When works councils lack the capacity to act, trade unions could step in to provide support and expertise to workers and their representatives at plant level. For instance, in Germany, IG Metall, the German metalworkers' union, has been very active on the (digital) transformation of the workplace, by providing training, technical expertise and resources to workers' representatives on the shop floor (see Infobox 14).

BOX 14: IG Metall and Industry 4.0

In its Work+Innovation programme, IG Metall, the German metalworkers' union, is helping works councils and shop stewards to effectively use their information and co-determination rights at the company to shape the technological transformation of work. The project focused on providing training, help with practical implementation of processes on the work floor, and support from a network of outside experts (academics, consultants).[77]

Trade unions also need to provide practical tools, which allow works councils to assess new technologies and influence the

processes. One such tool is the 'compass for digitalisation', which has been developed IG Metall, together with researchers.[78]

However, unionisation rates and trade union capacity vary widely across sectors and countries. Whereas in Nordic countries like Denmark, Finland and Sweden, trade union density stands at an average of 64.7 percent, this is much lower in other parts of the EU (see Table 2 in the following page).

---

76 T. Albrecht and C. Kellermann, 'Artificial Intelligence and the Future of the Digital Work-Oriented Society', Friedrich-Ebert-Stiftung, October 2020, at: https://socialdialogue.fes.de/news-list/e/artifical-inteliigence-and-the-future-of-the-digital-work-oriented-society
77 K. Schäfers and J. Schroth, 'Shaping Industry 4.0 on Workers' Terms'. IG Metall's Work_Innovation Project'.
78 T. Albrecht and D. Gerst, 'Designing Work in a Digitalising World', *Social Europe Journal* 18 May (2021), at: https://socialeurope.eu/designing-work-in-a-digitalising-world

No digitalisation without representation

Table 2: Trade Union Density across Europe (2018)

	North	Centre-West	South	West	Centre-East
Trade Union Density	64.7%	29.1%	19.1%	37.8%	27.1%
Countries	DK, FI, SE	AT, BE, DE, LU, NL, SI	ES, FR, GR, IT, PT	CY, IE, MT, UK	BG, CZ, EE, HR, HU, LT, LV, PL, RO, SK

Source: Torsten Müller, 'Collective Bargaining Systems in Europe. Some Stylised Facts', ETUI, 2020; based on OECD-AIAS ICTWSS Database (2020).

In addition, unions do not reach all workers. For instance, workers active in the platform economy are often treated as self-employed, whilst being subject to intricate forms of algorithmic surveillance and management. This means they lack the collective bargaining structures and protections that employees usually do have – at least in theory – when it comes to information, participation and co-decision power over new technology. For platform workers to understand how they are being managed and if they are being treated unfairly or discriminated against, it does not suffice to obtain individual data that is now possible – albeit still impractical – under the GDRP.

For instance, whereas individual Uber drivers may use the GDPR to get access to, and information about, personal data collected about them at work, the insights they can draw from that are limited. Only when they combine that with the data of other Uber drivers will they be able to gather actionable insights from the data.

Also for (prospective) employees, the scope of labour law may not be sufficient. For instance, employers may screen social media to gather information about specific individuals and draw conclusions about their employability and future performance, before a contract has ever been signed. Similarly, employers may track the type of browser job applicants use when carrying out online tests, to assess their future performance.[79]

7.3 Social partners at EU level: the Framework Agreement on Digitalisation

Given the pace of digitisation at the workplace, as well as the often global software firms that are pushing it, it could be expected that social partners at European level would take up the mantle and provide structural safeguards that would be difficult to realise for workers at the level of the individual firm. And indeed, the social partners at European level concluded a Framework Agreement on Digitalisation in June 2020.[80]

---

79 D. Peck, 'They're Watching You at Work', *The Atlantic*, December (2013), at: https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/

The document recognises that there are several challenges stemming from the digitisation of the workplace for work organisation, working conditions and skills, and encourages a 'partnership approach between employers, workers and their representatives', as well as the 'development of a human-oriented approach to integration of digital technology in the world of work'. However, the agreement does not provide binding interpretations of, for instance, the GDPR, nor clear guidance on how its provisions should be applied in the world of work. Instead, the specific challenges of digitisation are considered to be context dependent, and unsuitable to be tackled collectively at EU level.

The agreement covers four issues: digital skills and securing employment; modalities of connecting and disconnecting; artificial intelligence and guaranteeing the human-in-control principle; and the respect of human dignity and surveillance. Under each of these headers, **the agreement lists broad principles, and sets of voluntary measures to be considered, with little detail or prioritisation**.[81] Therefore, it is unlikely they will provide much practical help to workers' representatives at more decentralised levels.

The agreement focuses on process, whilst leaving the content to be negotiated in a decentralised fashion, at the workplace, or to a lesser extent via collective bargaining. The references to national procedures and practices mean that in practice a lot will depend on the legal guarantees in different member states for worker participation and co-determination, as well as the power and capacity of works councils and unions to demand a seat at the table. Unfortunately, as has been established,

the laws of different member states, as well as the effective capacity of unions and works councils, is highly variant between and within different member states of the EU.

> ### BOX 15: Tools for works councils
>
> In 2017, UNI Global Union developed 10 principles for workers' data rights and privacy. Together, they offer a framework for data governance in the workplace that can serve as guidance for unions and works councils across Europe.[82] In addition, the Why Not Lab has clarified the different phases of the data lifecycle, and their relevance for workers' representatives.[83]
>
> In 2021, AlgorithmWatch published guidelines to help works councils with their responsibility for reviewing AI-based systems that are being introduced in the workplace. The guidelines contain detailed questions on the functioning of the software, the way quality is ensured, and the way in which the new system is integrated into the firm.[84]

80   BusinessEurope, SMEunited, CEEP and the ETUC, 'European Social Partners Framework Agreement on Digitalisation', June 2020, at: https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf.
81   See also I. Senatori (2020) 'The European Framework Agreement on Digitalisation: a Whiter Shade of Pale?', *Italian Labour Law e-Journal* 13 (2) 2020.
82   UNI Global Union, '10 Principles for Workers' Data Rights and Privacy' (2017).
83   Christina Colclough, 'Workers' Rights: Negotiating and Co-governing Digital Systems at Work', *Social Europe* September (2020).
84   S. Stiller, J. Jäger and S. Gießler, 'Automated Decisions and Artificial Intelligence in Human Resource Management: Guideline for Reviewing Essential Features of AI-based Systems for Works Councils and Other Staff Representatives', 18 May 2021, AlgorithmWatch, at: https://algorithmwatch.org/en/wp-content/uploads/2021/05/AlgorithmWatch_AutoHR_Guideline_2021.pdf.

8. The EU legislative agenda – governing data and algorithms

The European Commission has realised that there are fundamental problems with the legal architecture around data. Right now, large tech firms are gobbling up data, but more beneficial forms of data-sharing lack explicit governance architecture to take off. Similarly, the European Commission acknowledges that some of the problems with algorithmic systems, notably concerns about safety and a lack of transparency and human oversight, require measures that go beyond the rights and obligations of the GDPR. Therefore, it has published a range of legislative proposals to increase access to data and improve the data governance ecosystem, as well as to build in safeguards for algorithmic systems on the EU market.

While these draft laws offer promising avenues for increasing protection of citizens and workers, they are unlikely to reach their intended purpose, because they do not foresee effective institutions to implement and enforce the law.

8.1 The Data Governance Act and beyond

Whereas large tech firms are aggregating the data of millions of citizens, with little transparency, the latter find it difficult to collectively represent their interests. Data protection laws allow enterprising individuals to gain access to their personal data, but they do not provide for the collective governance mechanisms that can provide more beneficial forms of data-sharing and countervailing powers. Workers – many of whom cannot rely on meaningful participation and information rights under labour laws – face a similar problem.

This is for example the case for platform workers, who are bereft of insights from data that can only be grasped in aggregate form. Whereas individual Uber drivers may use the GDPR to get access to, and information about, personal data collected about them at work, the insights they can draw from that are limited. Only when they combine that with the data of other Uber drivers will they be able to gather actionable insights. In addition, many gig platforms, such as Uber, use data from workers to train and improve their algorithms, which they then protect via intellectual property and trade secrecy laws.[85] As Professor Brishen Rogers puts it 'Uber has captured or replicated some of drivers' tacit knowledge and craft skills, which it now leases to drivers'.[86]

Addressing this would require forms of 'data stewardship'. According to Mozilla's Data Futures Lab, a data steward is an intermediary 'who manages data (rights) on behalf of beneficiaries within a consent-based structure and towards a defined goal'.[87] With the proposed Data Governance Act of 2020, the European Commission intends to facilitate the rise of such data intermediaries.[88]

BOX 16: Examples of data stewardship, Mozilla Data Futures Lab

Data cooperative: the collaborative pooling of data by individuals or organisations for the benefit of the group. A good example is Driver's Seat, a cooperative of private-car drivers who pool their data, to gain aggregate insights that would otherwise be only available to ride-hailing platforms like Uber, Lyft and Ola.

---

85   O. Lobel, 'The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property', *Texas Law Review* 93(789) (2015).

86   B. Rogers, 'The Law and Political Economy of Workplace Technological Change', *Harvard Civil Rights-Civil Liberties Law Review* 55 (2021), p. 562,

87   Mozilla Insights, 'Data Futures Lab Glossary', at https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/ data-futures-lab-glossary/.

88   European Commission, 'Proposal on European data Governance (Data Governance Act)', COM/2020/767 final.

89   J. van Geuns and A. Brandescu, 'Shifting Power Through Data Governance', September 2020, Mozilla Insights.

> **Data trusts:** a legal construct where a trustee manages data for the interests of a group of beneficiaries. Although the concept originates in common law countries (US, UK), the EU is aiming to introduce similar concepts at EU level, with the proposal for a Data Governance Act.

The Data Governance Act is still being negotiated, but it looks like it will introduce valuable concepts, such as data-sharing services, which must comply with fiduciary duties. That is, these new types of data steward must act in the best interest of those whose data they manage. This could lead to new and better business models for data-sharing. The proposal covers the sharing of personal data, although at present it does not allow for rights under the GDPR to be conferred or delegated to a data cooperative, which would likely hinder the effectiveness of the regulation, as data cooperatives cannot effectively represent their members, other than the limited options that the GDPR already allows.[90]

That said, the proposal does not address the governance issues that will likely arise from increased data-sharing. As Sean McDonald has explained, whereas the act lays down conditions for EU-wide market actors to provide data-sharing services, the task of supervising the implementation of these rules, as well as managing the political conflicts that will arise, are left to national institutions.[91] Most likely, this includes data protection authorities, which are already incapable of acquitting themselves of their current legal responsibilities.

The Data Governance Act does provide for a right to lodge a complaint against data-sharing service providers, as well as the right to an effective judicial remedy. However, these will ultimately have to be guaranteed by institutions that are already overburdened. Moreover, the only institution that is foreseen at EU level is the 'European Data Innovation Board'. This expert group has no binding authority and will have to rely on persuasion and informal pressure to ensure minimum standards across the EU. In the light of the experience with the GDPR, which has a stronger EU coordination mechanism, this is unlikely to be sufficient.

In sum, the Data Governance Act has the potential to stimulate more responsible business models around data-sharing and could help in particular gig economy workers to aggregate their bargaining power over data. At the same time, the lack of institutional complements, oversight and redress mechanisms may complicate the effective implementation of the law.

The proposed Digital Services and Digital Markets Acts generally neglect employment issues, but would add to the Digital Governance Act increased access to data from the very largest platforms, at least for competent authorities and in certain cases vetted researchers and business users. In addition, there will be transparency obligations about the terms and conditions of online platforms, as well as the algorithms and recommender systems they use. However, the requirements for data access and external auditing only apply to the very largest platforms, which will exclude most if not all gig economy platforms. Therefore, these legal proposals will not help uncover and address potential issues around systemic discrimination that may affect platform workers.

8.2 The regulatory framework for AI

The GDPR has not (yet) stimulated the creation and design of software that supports workers' rights over their data, as well as their autonomy and participation in a digitised working environment. Similarly, the systems for co-determination and participation of workers do not seem to be effectively translated into digital systems. There are many reasons for

---

90   European Commission, 'Proposal on European data Governance (Data Governance Act)', COM/2020/767 final, recital 24.
91   S. McDonald, 'A Novel, European Act of Data Governance', Centre for International Governance Innovation, 2020.

No digitalisation without representation

this, from weak rights and gaps in enforcement, to the lacking technical capacity of trade unions and the nature of algorithmic systems that are often cloud-based, frequently-tweaked and (deliberately) difficult to understand. Hence, the move to digital seems to exacerbate information asymmetries between workers and management.

Against that backdrop, the European Commission's proposed regulatory framework for AI is a promising initiative.[92] With the proposal, the Commission aims to increase the security of algorithmic systems and make them easier to understand, and to force developers and users to be more transparent about and accountable for the usage and implications of such systems. Coming in the form of a regulation, the future law would create direct legal obligations standards for all who operate, deploy or use AI systems that are considered high risk. When it comes to employment relations, however, the proposed regulation falls short. It only looks at developers and 'users', the latter usually being businesses and employers, without taking workers (and consumers) into account.

The legal framework classifies 'AI' systems that are used in the management of workers and access to self-employment as high-risk systems. This covers for instance the use of algorithmic and automated systems for the recruitment and firing of workers, and the allocation of tasks and monitoring of performance. According to the draft law, the classification of AI systems in the workplace as high risk means that the data used as inputs to the system need to be relevant and representative. In addition, it entails that such systems need to ensure adequate human oversight, also by facilitating this in their design.[93] The focus on the design of systems is reminiscent of the approach taken in the GDPR, which also requires data protection by design.

But it is not at all clear how to translate such abstract principles into a concrete reality.[94] For instance, the draft regulation requires high-risk systems to be designed in such a way that they can be effectively overseen by humans. In addition, data used for high-risk systems should be representative and relevant. But who will decide what is an appropriate design, and when data is representative? This would require close cooperation between stakeholders, like civil society and workers' representatives, the software industry, academia, and authorities. Yet that is not addressed in the legislation. In the absence of standards, rules and institutions, these questions are likely decided by employers and the software industry alone. Finally, one could ask whether crucial decisions like dismissals should be classified as high risk, instead of being excluded from automated decision-making at all.

Because the proposed 'AI Act' gives no concrete participation, consultation and complaints rights to workers and their representatives (or any citizens for that matter), the brunt of responsibility comes down to software developers and individual employers using AI systems in the workplace. They must self-assess and ensure compliance with regulations. But for instance with the GDPR, studies about the use of data protection risk-mitigation tools like data protection impact assessments, also a form of self-assessment, have shown gaps. These provisions lead to a range of compliance measures, but they do not address risks for data subjects, nor ensure the creation of software that is privacy friendly.[95] Similarly, it can be expected that self-assessment under the future AI rules will focus on reducing firms' exposure to liability, without meaningfully engaging with workers' needs.

Of course, as has been previously analysed, existing labour laws across Europe already provide a measure of protection against some of the risks of algorithmic systems in the workplace – however patchy and imperfectly. And yet, because the

---

92   European Commission, 'Proposal for an Artificial Intelligence Act', COM/2021/206 final.
93   European Commission, 'Proposal for an Artificial Intelligence Act', Articles 10 and 14, 2021.
94   See for instance M. Coeckelbergh, *AI Ethics* (London: MIT Press, 2020), 165.
95   F. Ferra, I. Wagner, E. Boiten et al, 'Challenges in Assessing Privacy Impact'.

draft AI rules are coming in the form of a directly applicable regulation, without a reference to social partners and existing national protections around algorithmic management, some experts fear this may undermine existing and more stringent national rules and labour practices.[96] Whereas in certain jurisdictions the introduction of intrusive new surveillance and control technology would require detailed governance agreements concluded with labour representatives, the AI Act in its current form seems to open the door for such systems, based on a light form of self-assessment.

This does not mean the EU should not put forward binding rules on automated decision-making systems: it should. In particular given that collective bargaining is weak or practically absent in large parts of Europe, minimum conditions for the usage of such systems that interact with workers are necessary. But – as is clear from the current legal base, which is market integration – the EU should not create a situation where EU-wide market integration and the spurring on of the adaption of AI, combined with a soft self-assessment regime, leads to the displacement of local collective action that shapes how the rules should be interpreted in the workplace.

This is even more so given that the new AI rules do not foresee strong enforcement, or an EU-wide body for joint action and coordination. The foreseen European Artificial Intelligence Board is a mere expert group, with no decision-making power or significant staff; and as M. Veale and F. Borgesius noted, 'arcane electrical standardisation bodies with no fundamental rights experience [are] expected to write the real rules'.[97] In a similar vein, they note that the market surveillance bodies tasked with enforcement are ill-equipped to handle the vast task of overseeing not just AI developers, but also users, in a variety of different contexts. The chances that

the authorities will be able to take on such complex new responsibilities are infinitesimal.

Therefore, it is crucial that the coming proposal on artificial intelligence is accompanied by institutional mechanisms to bridge the gap between those who design systems and communities that will face the consequences, not least in the workplace.

8.3 Who designs, decides: influencing software development

It is 20 years since US law professor Lawrence Lessig prophesied that code is law, and that citizens and collective institutions should decide the shape of digital infrastructure.[98] As workplace relations are increasingly codified – and obscured – in systems that manage by algorithm, his dictum is especially relevant for the world of work.

Whereas workers are still struggling to make use – defensively – of data protection rights, today's algorithmic systems pose a much broader risk, and an opportunity. Right now, the opportunity to gather, store and analyse massive quantities of data allow firms to get a real-time picture of production processes, a 'digital twin', that can be used to steer and optimise tasks with almost instant feedback. In Europe, this is for instance what companies like Celonis promise.[99]

The question is what that intelligence will be used for. The trend indicates a continuation of the Taylorist revolution – with novel means. Workers are increasingly monitored and controlled, which undercuts their autonomy and bargaining power. However, alternatives are possible. Even in the early 1970s, Stafford Beer, cybernetic visionary and management consultant, advised the Chilean government on how to build a technological system

---

96   V. De Stefano, 'The EU Proposed Regulation on AI: A Threat to Labour Protection?'. Regulating for Globalization, Wolters Kluwer, 16 April, 2021 at: http://regulatingforglobalization.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/.
97   M. Veale and F. Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act', *Computer Law Review International* 22(4) (2021).
98   L. Lessig, *Code and Other Laws of Cyberspace* (New York, Basic Books, 1999).

No digitalisation without representation

to track and manage production: Project Cybersyn. It was algorithmic management at national scale.

However, it was not devised as a system facilitating technocratic control. As scholar Eden Medina explains, Stafford Beer recommended that 'the government allow workers – and not engineers – to build the models of state-controlled factories because they were best qualified to understand operations on the shop floor. Workers would thus help design the system that they would then run and use. Allowing workers to use both their head and their hand would limit their feelings of alienation from their labor.'[100]

<div style="background:#c8102e; color:white; padding:1em;">

BOX 17: Project Cybersyn

The Cybersyn project 'showed an ability to envision how computerization in a factory setting might work toward an end other than speed-ups and deskilling […]. The state created the conditions for new directions in design thinking by making social justice a priority and providing financial and human resources to push technological innovation in this direction. It shows that the state can require (and inspire) technologists to consider how systems benefit the interests of the broader citizenry, which may or may not align with profit, market success, efficiency, technical elegance, or coolness in system design.'[101]

</div>

Following the aim to increase worker influence over the design of software, what would be necessary today is that workers' interests and official representative functions are directly embedded in algorithmic systems themselves; to include functionality that allows works councils and shop stewards to automatically have access to relevant information, for instance to ensure – directly – that labour laws and workers' rights are respected, for instance on overtime, or the prohibition against discrimination. While trade unions already fight for access to digital communication networks, they might as well demand access to digital management systems and 'digital twins'. This thinking is already evident when it comes to environmental sustainability. For instance, software provider SAP has already announced it is aiming to integrate the full ecological footprint of anything that runs through its Enterprise Resource Planning system (ERP). Hence, in this case, software is explicitly designed to facilitate sustainability. To ensure a socio-ecological transition, something similar should happen for social requirements. This is in line with the EU's official policy goals, which aim to combine both the social and environmental agendas.[102]

However, it is unlikely that large software providers will design systems for social sustainability and worker empowerment of their own accord. The fact that such a shift is – slowly – taking place for the green transition clearly happens because providers anticipate binding legislation in the wake of the social mobilisation of the past years, as well as a developing business case in going green.

In the past there have been experiments and programmes to involve workers in the design of technology, especially in the Nordic countries. Very successful was a certification scheme for computer hardware – called TCO – that was initiated by the Swedish Confederation of Professional Employees in 1992.[103] For software, the Swedish Trade Union, together with the Swedish Confederation for Professional Employees, launched the UsersAward

---

99   Cracked Labs, 95.
100   E. Medina, 'Rethinking Algorithmic Regulation, *Kybernetes* 44(6–7) (2015), 1010.
101   Ibid, 1010.
102   See for instance European Commission, 'Communication on a Strong Social Europe for Just Transitions', COM (2020), 14.
103   A. Walldius et al, 'User Certification of Workplace Software: Assessing both Artefact and Usage', *Behaviour & Information Technology* 2(28) (2019), 101–20.

Programme in 1998. It included user surveys in specific industries, conferences, design projects, IT prize contests, and the creation of a certification scheme for workplace software.[104]

However, after an initial certification of two software packages in 2002, the scheme never really took off, in part due to reactiveness and a lack of cooperation with software providers.[105] Engaging software providers today is likely even more difficult, given the concentration in many market segments of business software. Given that much of the workplace software systems are provided by large firms that deliver for the entire EU market and beyond, the social contest over their design cannot take place exclusively at the level of the individual firm, or even at national level. It will require an institution that operates across the EU, and that bundles the expertise and networks of trade unions, civil society organisations, academia (data protection and labour law, human–computer interaction, software engineering) and relevant public authorities.

Such an institution should bundle the expertise and capacity to certify software packages and updates. One could think, for instance, of a certification scheme, where software would be tested ex ante, and labelled as GDPR and labour law compliant. The timing is apposite, as in many areas – from how to implement the GDPR in the workplace context, to future rules for human-centric design of AI systems – no certification or standards exist. In addition, current standards bodies often lack the legitimacy and mechanisms that would allow civil society and social partners a meaningful influence.[106] This would provide security for workers and works councils, as they could now easily ask employers for a compliance certificate. But it would also benefit the firms developing and using the software, as they would gain the certainty that their systems are at a

minimum legal, and ideally also user-friendly. Such an institution could also be involved in the auditing of software already on the market, possibly enabled by provisions under the future Digital Markets and Services Acts.

---

104   A. Walldius, J. Gulliksen and Y. Sundblad, 'Revisiting the UsersAward Programme from a Value Sensitive Design Perspective', 5th Decennial Aarhus Conference on Critical Alternatives, 2017.

105   J. Larner and A. Walldius, 'The Platform Review Alliance Board: Designing an Organizational Model to Bring Together Producers and Consumers in the Review and Commissioning of Platform Software', *Journal of Organization Design* 14(8) (2019).

106   J. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019), 202-237.

RECOMMENDATIONS: INCREASING INSTITUTIONAL CAPACITY

RECOMMENDATIONS: INCREASING INSTITUTIONAL CAPACITY

The GDPR offers workers and their representatives significant means to gain insights into the collection and use of their personal data, and some means to get access to ensuing analysis and decisions being taken based on that. Existing information and participation rights for labour provide an even broader scope for workers to be informed of – and involved in – the deployment of new technology in the workplace. However, for these rights to translate into tangible outcomes, a vast effort needs to be made to improve existing oversight institutions and the capacity of collective institutions that represent labour at national and firm level.

EU institutions and member states:

• Data protection authorities (DPAs) should receive proper human and financial resources, as well training in the application of the GDPR to workplace contexts. In a digital economy, the protection of personal data is no longer a niche concern, rather a fundamental consideration in each workplace. The capacity of regulators should reflect this.

• Member states that have not done so should implement the option for collective action under Article 80(2) of the GDPR, to alleviate some of the burden on individuals and DPAs, and allow more trade unions and civil society organisations to provide collective enforcement of individual data protection rights.

• EU institutions should prioritise labour interests in proposals such as the Data Governance Act, and especially the AI Act, and enable thorough auditing infrastructures in both laws. The AI Act places too much trust in the assessment of compliance by firms themselves. It needs to explicitly enable works councils and unions to play their part in overseeing the introduction of algorithmic systems in the workplace.

• The European Commission's announced proposal to improve working conditions of platform workers should establish platform workers' right to collective bargaining.

Data protection authorities:

• Employment should be a priority area for DPAs, especially in view of the boom in digitisation in the wake of the Covid-19 pandemic. This is an area where early intervention is still possible, and where regulators can help set expectations and shape practices, instead of intervening once an entire business model has crystalised around unsustainable practices (as happened with consumer-facing online platform services).

• DPAs need increased funds to carry out systematic information, advice and enforcement campaigns on data protection in the workplace. In particular given the rapid changes in the wake of the Covid-19 pandemic, there is an urgent need for and clear benefit from ex officio enforcement action and guidance activities.

• Given the lack of enforcement resources, the few decisions taken by DPAs around employment should be aimed at creating wider pedagogic and dissuasive effects. This means fewer informal negotiations behind closed doors and more reliance on official published decisions coupled with effective fines.

• A special database, available to the public, should be created on DPAs' decisions relating to the workplace and related court decisions, thus spreading knowledge and best practices to all involved, including unions, works councils, employers and producers of data systems used at the workplace. In the medium term, such a database will significantly reduce the workload

of DPAs in this area, as it will allow conflicts and litigation to be avoided, if interpretations and expectations are stabilised and become foreseeable through publicity given to the practice of DPAs and courts.

Trade unions, shop stewards and works councils

- In the face of signs of widespread illegal use of workers' data, shop stewards and works councils should fill gaps in worker knowledge on data protection rights, actively represent workers' data protection interests with regard to management, and help workers to lodge complaints. DPAs are obliged to follow up on complaints about alleged non-compliance with the GDPR.

- Works councils, unions and shop stewards should seek the cooperation of the data protection officer (DPO) responsible for the workplace. Together, they should be involved in all major steps of the deployment of technological systems that process personal data. The DPA can also be an important partner in explaining the relevance of the GDPR for the workplace.

- Each trade union should have a data analyst within their ranks, or collectively accessible. Without expertise on data and algorithmic management – both legal and necessarily also technical – unions will struggle to remain relevant in this field. Inversely, by seizing the moment and actively supporting data protection claims from works councils, shop stewards and individual workers, unions can play an important role in improving the workplace of tomorrow.

- Given the lack of interpretation of key GDPR provisions for the workplace, unions should aim to adopt collective agreements enabled by Article 88 of the GDPR; in addition, they should spur on clarification of the GDPR by bringing test cases to court. In addition, unions can encourage academics to provide the necessary interpretation. The modern workplace needs closer cooperation between labour and data protection lawyers, and

unions should drive the closer cooperation of these two fields.

- At EU level, trade unions should create a methodology that would allow unions and works councils to measure how well they are able assert their constituents' rights on digital technology questions. This could help identify skills and capacity gaps. The social dialogue institutions should seek a systematic dialogue with the European Data Protection Board.

- The design of software is crucial, but difficult to influence as developers often operate globally and use IP and trade secrecy laws to prevent scrutiny of their software. Trade unions and civil society, in collaboration with universities and public authorities, should set up a new institution that operates across the EU, and which would facilitate the certification and auditing of software systems for the workplace, from a worker perspective.

BIBLIOGRAPHY, AUTHORS, ABOUT FEPS & PARTNERS

BIBLIOGRAPHY

Adams-Prassl, J. 'What if your Boss was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work', *Comparative Labor Law & Policy Journal* 41(1) (2019).

Albrecht, T., and C. Kellermann, 'Artificial Intelligence and the Future of the Digital Work-Oriented Society', Friedrich-Ebert-Stiftung, October 2020, at: https://socialdialogue.fes.de/news-list/e/artifical-inteliigence-and-the-future-of-the-digital-work-oriented-society.

Albrecht, T., and D. Gerst, 'Designing Work in a Digitalising World', *Social Europe Journal* 18 May (2021), at: https://socialeurope.eu/designing-work-in-a-digitalising-world.

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

Article 29 Working Party (2017) WP 248, 4 April 2017, at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2017.

Aloisi, A., and E. Gramano, 'Artificial Intelligence is Watching you at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context', *Automation, Artificial Intelligence & Labor Law* 41(1) (2019).

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), 'AP: Verwerking gezondheidsgegevens wearables door werkgevers mag niet' (8 March 2016), at: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet.

Autoriteit persoonsgegevens, 'Jaarverslag 2020' (2021), at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf.

Berg, J. 'Protecting Workers in the Digital Age: Technology, Outsourcing and the Growing Precariousness of Work', SSRN (2019), at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413740.

Bronowicka, J. et al, *'Game that you Can't Win'? Workplace Surveillance in Germany and Poland* (Frankfurt (Oder): European University Viadrina, 2020).

Bundesarbeitsgericht, 27 July 2017, 2 AZR 681/16.

BusinessEurope, SMEunited, CEEP and the ETUC, 'European Social Partners Framework Agreement on Digitalisation', June 2020, at: https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%20_Agreement%20on%20Digitalisation%202020.pdf.

Bygrave, L. A., 'Article 22', in eds C. Kuner, L. A. Bygrave and C. Docksey, *Commentary on the EU General Data Protection Regulation* (Oxford: Oxford University Press, 2019).

Bygrave, L. A., 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making', University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2019-01, 2019.

CMS, 'GDPR Enforcement Tracker', at: https://www.enforcementtracker.com.

CNV, 'Half miljoen thuiswerkers via software in de gaten gehouden', at: https://www.cnv.nl/nieuws/half-miljoen-thuiswerkers-via-software-in-de-gaten-gehouden/.

Coeckelbergh, M., *AI Ethics* (London: MIT Press,

2020), 165.

Cohen, J., *Between Truth and Power. The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019).

Colclough, C., 'Workers' Rights: Negotiating and Co-governing Digital Systems at Work', *Social Europe* September (2020).

Cracked Labs, 'Digital Überwachung und Kontrolle am Arbeitsplatz. Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management?' (September 2021).

Dagnino, E., and I. Armaroli, 'A Seat at the Table: Negotiating Data Processing in the Workplace', *Comparative Labor Law & Policy Journal* (2020), 173–95.

De Loecker, J., and J. Eeckhout, 'Global Market Power', NBER Working Paper 24768 (2018).

De Stefano, V., 'Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection', *Comparative Labour Law & Policy* 41(1) (2019).

De Stefano, V., 'The EU Proposed Regulation on AI: A Threat to Labour Protection?'. Regulating for Globalization, Wolters Kluwer, 16 April, 2021 at: http://regulatingforglobalization.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/.

Ellguth, P., 'Ost- und Westdeutschland nähern sich bei der Reichweite der betrieblichen Mitbestimmung an', IAB-FORUM, 13 May 2020, at: https://www.iab-forum.de/ost-und-westdeutschland-naehern-sich-bei-der-reichweite-der-betrieblichen-mitbestimmung-an/.

European Commission, SWD (2020), 115.

European Commission, 'Digital Compass 2030' (2021), COM/2021/118 final.

European Data Protection Board, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities', 26 February, 2019, 7, at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.

Ferra, F., I. Wagner, E. Boiten et al, 'Challenges in Assessing Privacy Impact: Tales from the Front Lines', *Security and Privacy* 3(2) (2020).

Frey, C. B., *The Technology Trap: Capital, Labor, and Power in the Age of Automation* (Princeton: Princeton University Press, 2019).

Gürses, S., and J. van Hoboken, 'Privacy After the Agile Turn', in eds Evan Selinger et al, *Cambridge Handbook of Consumer Privacy* (Cambridge: Cambridge University Press, 2018).

Hendrickx, F., E. Gramano and D. Mangan, 'Privacy, Data Protection and the Digitalisation of Work: How Industrial Relations Can Implement a New Pillar', Kluwer Regulating for Globalization Blog, 26 June 2020, at: http://regulatingforglobalization.com/2020/06/26/privacy-data-protection-and-the-digitalisation-of-work-how-industrial-relations-can-implement-a-new-pillar/.

Holmberg, S. 'Fighting Short-Termism with Worker Power', Roosevelt Institute (17 October 2017).

Humphries, J., 'The lure of aggregates and the pitfalls of the patriarchal perspective: a critique of the high wage economy interpretation of the British industrial revolution', *Economic History Review* 66 (3) (2013).

Huws, U., N. Spencer and M. Coates, 'The Platformisation of Work in Europe. Highlights from Research in 13 European Countries', FEPS, UNI Europa and the University of Hertfordshire, 2019.

Information Commissioner's Office, 'How Do We Do a DPIA?', at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7.

Kress, C., R. Van Eijk and G. Zanfir-Fortuna, 'New

Decade, New Priorities: A Summary of Twelve European Data Protection Authorities' Strategic and Operational Plans for 2020 and Beyond', Future of Privacy Forum, 12 May 2020, at: https://fpf.org/wp-content/uploads/2020/05/FPF_DPAStrategiesReport_05122020.pdf.

Larner, J., and A. Walldius, 'The Platform Review Alliance Board: Designing an Organizational Model to Bring Together Producers and Consumers in the Review and Commissioning of Platform Software', *Journal of Organization Design* 14(8) (2019).

Leicht-Deobald, U., et al, 'The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity', *Journal of Business Ethics* 160 (2021).

Lessig, L., *Code and Other Laws of Cyberspace* (New York, Basic Books, 1999).

Lobel, O., 'The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property', *Texas Law Review* 93(789) (2015).

Mantelero, A., 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection', *Computer Law & Security Review* 32 (2017), 238–55.

McDonald, S., 'A Novel, European Act of Data Governance', Centre for International Governance Innovation, 2020.

Medina, E., 'Rethinking Algorithmic Regulation, *Kybernetes* 44(6–7) (2015).

Mendoza, I., and L. A. Bygrave, 'The Right Not to be Subject to Automated Decisions Based On Profiling', in eds T. Synodinou, P. Jougleux, C. Markou and T. Prastitou, *EU Internet Law: Regulation and Enforcement* (Springer: 2017), 77–98.

Moore, P. V., M. Upchurch and X. Wittaker (eds), *Humans and Machines at War: Monitoring, Surveillance and Automation in Contemporary Capitalism* (London: Palgrave Macmillan, 2018).

Noble, D. F., 'Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools', in eds D. Preece, I. McLoughlin and P. Dawson, *Technology, Organizations and Innovation: Critical Perspectives on Business and Management. Volume 1: The early debates* (London: Routledge, 2000)..

Nogarede, J., 'Governing Online Gatekeepers: Taking Power Seriously', FEPS, 2021.

NOS, '"Gluurappartuur" in trek door thuiswerken, vakbond bezorgd', at: https://nos.nl/artikel/2375956-gluurapparatuur-in-trek-door-thuiswerken-vakbonden-bezorgd.

Noyb, 'Luxemburg's Watchdog Refuses to Show its Teeth to US Companies', 25 January, at: https://noyb.eu/en/luxemburgs-watchdog-refuses-show-its-teeth-us-companies.

Nurski, L. 'Algorithmic Management is the Past, Not the Future of Work', blog post 6 May 2021, Bruegel, at: https://www.bruegel.org/2021/05/algorithmic-management-is-the-past-not-the-future-of-work/.

Pasquale, P., *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Cambridge, MA: Belknap Press, 2020).

Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information* (London: Harvard University Press, 2016)

Peck, D., 'They're Watching You at Work', *The Atlantic*, December (2013), at: https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

Prospect, 'Union Reveals that Half of Workers Don't Know What Data their Boss Collects About Them', 12 February, 2020, at: https://prospect.org.uk/news/union-reveals-that-half-of-workers-dont-know-what-data-their-boss-collects-about-them/.

Rechtbank Amsterdam, Uitspraak 11-3-2021, c/13/689705.

Richardson, R. 'Defining and Demystifying

Automated Decision Systems', *Maryland Law Review* 81 (forthcoming 2022).

Rogers, B., 'The Law and Political Economy of Workplace Technological Change', *Harvard Civil Rights-Civil Liberties Law Review* 55 (2021).

Ryan, J., and A. Toner, 'Europe's Enforcement Paralysis. ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities', Irish Council for Civil Liberties (2021).

Sarpong, S., and D. Rees, 'Assessing the Effects of 'Big Brother' in a Workplace: the case of WAST', *European Management Journal* 32(2) (2014).

Schäfers, K., and J. Schroth, 'Shaping Industry 4.0 on Workers' Terms. IG Metall's Work_Innovation Project', Trade Unions in Transformation 4.0 series, Friedrich-Ebert-Stiftung, September 2021.

Selbst, A. D., and J. Powles, 'Meaningful Information and the Right to Explanation', *International Data Privacy Law* 7(4) (2018).

Senatori, I., (2020) 'The European Framework Agreement on Digitalisation: a Whiter Shade of Pale?', *Italian Labour Law e-Journal* 13 (2) (2020).

Skillcast (2020), 'Remote-working Compliance YouGov Survey', 25 November, at: https://www.skillcast.com/blog/remote-working-compliance-survey-key-findings.

Staab, P., and S. Geschke, 'Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando', Study 429, Hans Böckler Stiftung (2020).

Stiller, S., J. Jäger and S. Gießler, 'Automated Decisions and Artificial Intelligence in Human Resource Management: Guideline for Reviewing Essential Features of AI-based Systems for Works Councils and Other Staff Representatives', 18 May 2021, AlgorithmWatch, at: https://algorithmwatch.org/en/wp-content/uploads/2021/05/AlgorithmWatch_AutoHR_Guideline_2021.pdf.

Stolton, S., 'Employers Accused of Abusing EU Data

Privacy Rules to Hinder Trade Unions', Euractiv, 19 March (2020).

Todolí-Signes, A., 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection', ETUI, 2019.

UNI Global Union, '10 Principles for Workers' Data Rights and Privacy' (2017).

Van Geuns, J., and A. Brandescu, 'Shifting Power Through Data Governance', September 2020, Mozilla Insights.

Veale, M., and L. Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling', *Computer Law & Security Review* 34(2) (2018).

Veale, M., and F. Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act', *Computer Law Review International* 22(4) (2021).

Viljoen, S., (forthcoming), 'Democratic Data: A Relational Theory For Data Governance', *Yale Law Journal*.

Walker, P., 'Call Centre Staff to be Monitored via Webcam for Home-Working "Infractions"', *The Guardian*, 26 March, 2021, at: https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions.

Wachter, S., and B. Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review* 2 (2019).

Wachter, S., B. Mittelstadt and L. Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law* 7(2) (2017).

Walldius, A., et al, 'User Certification of Workplace

Software: Assessing both Artefact and Usage', *Behaviour & Information Technology* 2(28) (2019), 101–20.

Walldius, A., J. Gulliksen and Y. Sundblad, 'Revisiting the UsersAward Programme from a Value Sensitive Design Perspective', 5th Decennial Aarhus Conference on Critical Alternatives, 2017.

Winner, L., 'Do Artifacts Have Politics?', *Daedalus 121* (1980).

ABOUT THE AUTHOR

JUSTIN NOGAREDE

Justin Nogarede is Digital Policy Analyst at Foundation for European Progressive Studies (FEPS). Previously, he worked in the Secretariat-General of the European Commission, among others on digital and single market policy files. Within the European Commission he was involved in the mid-term review of the Digital Single Market Strategy, and in policy on standard-essential patents, audio- visual media, internet governance and product liability.

ABOUT THE FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES (FEPS)

The Foundation for European Progressive Studies (FEPS) is the think tank of the progressive political family at EU level. Its mission is to develop innovative research, policy advice, training and debates to inspire and inform progressive politics and policies across Europe.
FEPS works in close partnership with its 68 members and other partners -including renowned universities, scholars, policymakers and activists-, forging connections among stakeholders from the world of politics, academia and civil society at local, regional, national, European and global levels.

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES

Avenue des Arts 46, B-1000 Brussels, Belgium +32 2 234 69 00
info@feps-europe.eu
www.feps-europe.eu
@FEPS_Europe

Power in the workplace is increasingly embedded in – and exercised through – the way data is collected and then used via algorithmic systems. This trend has received a boost during the Covid-19 pandemic. While this shift can – in theory – support the quality of work, at present it seems to mainly facilitate expanding surveillance and control of the workforce. To ensure a digital transition that is socially sustainable, workers and their representatives need to help shape the digital infrastructure that determines how they carry out their work. The early involvement of labour in the design and procurement of digital productivity tools will incentivise the producers of such systems to design them with workers' wellbeing in mind.

After a short overview of current trends and potential risks surrounding data-driven algorithmic systems, this paper analyses different policy areas where EU and national institutions, trade unions and civil society organisations can act to empower workers. After looking at the potential and limitations of the General Data Protection Regulation, the paper explores the role of collective information, participation, and co-determination rights of organised labour. Finally, the potential impact of future EU laws on the digital economy are analysed, as well as what can be done to ensure workers' influence over the design of software systems for the workplace.

The paper concludes with a set of policy recommendations for EU institutions and member states, data protection authorities, and the labour movement, with an emphasis on how to realise the potential of the General Data Protection Regulation (GDPR) for amplifying workers' voice in the digital transformation of work.