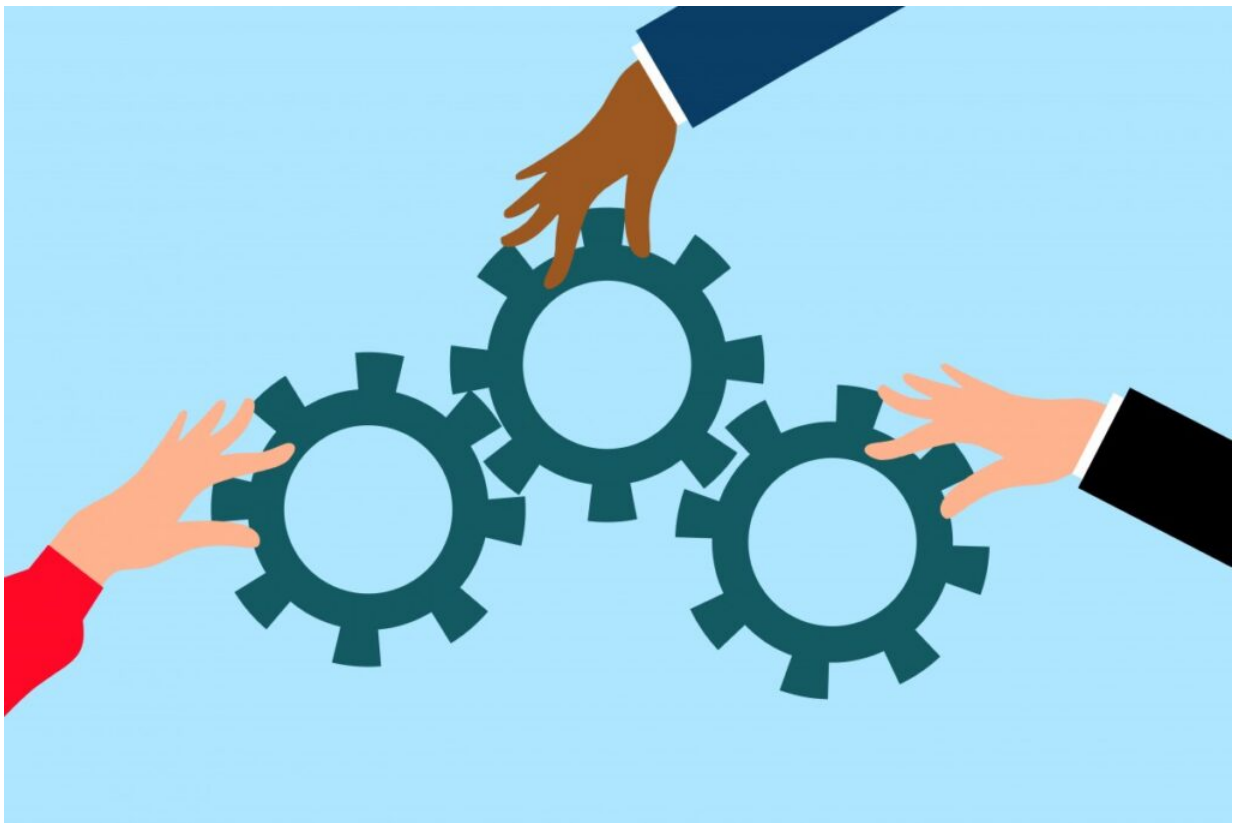


# Global Workplace Law & Policy

## Governing data, governing technology? Complementary approaches for the future of work

Michele Molè (University of Groningen) · Wednesday, November 23rd, 2022



### *David and Goliath: workers' data rights vs a vast market of surveillance*

An employer today can learn about interactions among employees or with customers via sensors and a vast variety of softwares. Is the tone of voice friendly enough with customers? How much time is spent on emailing or away from the assigned desk? Scores, 'idle' or silent buttons, are making the workplace a place where data is constantly accumulated and processed through Artificial Intelligence (AI) and the Internet of Things (IoT). Breaks can lead to penalties, from reduced bonuses to more serious sanctions [1]. These are just examples that represent strong evidence in the labour law debate: the recourse to data is changing organisational models and increasing employers' capability to monitor the workforce [2]. Thus, the self-determination and purpose limitation principles offered by the current General Data Protection Regulation (EU Reg 2016/679) are now standing under the magnifying glass: can they preserve the order of powers in

subordinate employment that datafication is disrupting? Or does guaranteeing individual rights against a vast and complex surveillance society risk creating an unequal David-and-Goliath conflict? [3]

This contribution suggests that data protection law at work is and will be crucial in ensuring labour protection in datafied workplaces. The present focus, however, is dominated by AI and IoT needs to be complemented with the governance of technologies (thus not only of data flows) that place structural limitations on employees' fundamental freedoms. A complementary approach that can be already recognised in the European Commission's Industry 5.0 strategy, with the proposal for a regulation on artificial intelligence as one of the main (yet problematic) developments [4].

### ***From Article 8 ECHR to GDPR: privacy at work as individual protection.***

Collecting and processing data at work is, in first place, a practical necessity and, subsequently, a fundamental element of an employment contract. The European Court of Justice (ECJ) has described it as a key feature of employment: subordinate employment is structured on hierarchies [5], and hierarchies function 'by superordinate positions monitoring and controlling positions below them in the hierarchy' [6]. Thus, to run a business an employer can collect data, for example, on employees' activities on corporate devices or accesses to corporate premises to check their working shift attendance [7].

To cope with a new era of data collection and processing, labour regulation has become increasingly intertwined with privacy and data protection law to fulfil its ultimate scope: balancing employers' economic aims with human dignity, social justice and decent work. Due to the fact that privacy and data protection ensure the development of personal space and identity, such rights have been assiduously described as 'the foundation from which all the other human rights and freedoms flow' [8]. This conceptualisation – i.e. a precondition to the other essential freedoms at work – gained prominence from the well-known *Niemietz v. Germany* (1992) before the Strasbourg Court. Safeguarding privacy and personal data at work under art. 8 ECHR became the channel to protect the working individual against a workplace increasingly scanning behaviours, results, and personal traits of the employee. An individual right to personal development and to establish relationships with other individuals at work, are after all, according to the Court, essential for the social life for most people, providing for a meaningful opportunity to build up connections with the outside world [9]. Hence, transparency, fairness and accountability of data collection and processing are the core principles that have been guiding the scholarship, courts, and legislators in reconciling the rising of the digitised workplace with the protection of the individual sphere of the employee [10]. The GDPR grants under those principles rights for individuals and duties for data controllers, turning the processing of employees' personal data co-ordinated and controlled (involving also third parties other than the employee and the employer, such as the Data Protection Officer or the European Data Protection Board). The current EU framework on data thus expresses an understanding of privacy pertaining to the control of one's own information by means of 'selected disclosures' and partly by guaranteeing the inaccessibility to a data controller of certain categories of data (such as sensitive data), or by limiting the purposes of data processing (art. 5, 6, 9 GDPR). In short, individuals and employees, being the source or owners of personal data, have guaranteed principles and rights to protect the integrity of their personality [11].

### ***The Datafication of the workplace: is data protection enough?***

A growing research, however, is pointing out how applying the GDPR's individual approach

reliant on controlling information and guaranteeing intimacy risks falling short of the goal of art. 8 ECHR protection and of other fundamental labour rights (such as a right to equal treatment, association, assembly) [12]. Indeed, a vast market of surveillance and human resources management products is slowly adding, step by step, additional capabilities to the employer's authority. Organisations today rely on a greater volume of data, mostly collected to learn how people relate to each other and to reveal additional characteristics: how we are in our interpersonal relationships with colleagues, how my tone of voice on the phone appeals to customers compared to that of my colleagues, and so on [13]. Securing control over one's own information, and then labour rights, comes increasingly at loggerheads with the creation of complex 'patterns of behaviour, identified as amalgams of categories or classifications (...), violating basic notions of individuals as autonomous beings' [14]. To this rapid flow of workforce patterns and classifications, the GDPR opposes a proprietarian and dignitarian view of the collection and processing of personal data; individuals, as the sources of personal data, have the right to protect themselves and to know how their identities are being used by the State or a private individual such the employer. On the data controllers' side, in principle, any data collection or processing may be legitimate, if lawfulness, fairness and transparency, purpose limitation and the other principles applicable to processing are being applied [15]. In short, the legislator through the GDPR is not addressing the social impact that technological development has on datafication processes; it lacks a tight mesh on the legality and legitimacy of data collection and processing in the workplace, where economic and contractual necessities can substantially legitimise the vast majority of software for management and surveillance [16]

In this context the software and hardware market has been able to graft more and more invasive and complex products onto the employer's authority. This graft was boosted by letting data protection at work be based on consent, in a contractual relationship with strong negotiation asymmetries; but also through rights to be informed in favour of employees with no knowledge on how to rectify unjust and unlawful data uses. So much so that today we are discussing how privacy guarantees are being eroded; or, in other words, are failing in their traditional function of limiting the collection and processing of personal data; with great concern for the social effects – both in the workplace and in the citizen/institution relationship. Appropriately addressing the contemporary social consequences of digital technologies requires a social scope of data protection. And thus, rethink how we conceptualise the legitimate and illegitimate production of information today [17].

### ***Forthcoming regulatory approaches at the EU level: complementing the GDPR with a 'social' scope of digital technologies development***

Rethinking socially responsible data protection is a complex task that cannot be accomplished here. Today, however, a different regulatory approach to digitisation at the European level is noticeable for the first time. In spring 2021, as part of the Industry 5.0 strategy of the European Commission, was published a proposal for a regulation to harmonise the rules on Artificial Intelligence [18]. The Commission's Industry 5.0 strategy introduces in fact interesting elements. Such agenda aims to overcome a market-driven view of digitalisation at work in favour of regulatory approaches that value workers well-being [19]. To this end, the proposed regulation adopts a classification system for uses of Artificial Intelligence; including prohibited implementations, up to the identification of high-risk uses. For high-risk uses, a series of third-party assessments are foreseen, with obligations to comply and conduct risk assessments, transparency obligations, human oversight, accuracy, robustness and cybersecurity. Employment falls within the latter classification, framing hiring and termination of employment contracts, monitoring and evaluating performances and behaviours as

high risk implementations of AI. Prohibited practices, on the other side, concern more the use of social scoring by public authorities and biometric recognition in public spaces [20]

The intention of the European legislator is to create a normative framework to hold bad actors accountable and to enable market players demonstrating that AI is legal and safe. The inclusion of both ex-ante and ex-post evaluations takes into account the fact that AI products evolve and update their internal decision-making logic over time. Impact evaluations would thus help to create a traceable record and positively filter out developers who design and deploy autonomous workforce management and surveillance systems.

With this proposal the European Commission for the first time focuses on the regulation of a specific technology, complementing the GDPR. It does not focus on data flows, but addresses precisely that dimension missing from the GDPR to date: the social impact that some new technologies processing personal data have. This complementarity inspired by the Industry 5.0 strategy, in principle, paves the way to overcome the short-circuit of data protection applied as social protection: that is, the affirmation of a civil right of selfhood in place of a social protection that would curb a market relentlessly searching for more meticulous products to be sold to employers [21].

Reforming the GDPR in relation to employment is perhaps too early. Adapting the EU regulation on data protection to employment contexts is nevertheless possible through Article 88 GDPR, which allows Member states to implement more employee-friendly legislations regarding the collection and processing of data at work. In recent years, however, this ‘open clause’ for labour contexts has shown some fragmentation and little involvement of social partners [22]. The most relevant normative approach in recent years yet remains the one taken by the European Commission with the proposal for a European AI regulation. I share the non-positive opinion of those who believe that the current proposal of the regulation may lower labour protections or get in the way of national regulations and social partners [23]. Many national legislations, e.g. the Netherlands, Germany, Italy require the involvement of trade unions and works councils before introducing management and surveillance technologies. The draft regulation does not mention the social partners in any specific way, thus already causing a certain degree of legal uncertainty. Will they still have a role when AI is implemented at work? [24]. Moreover, banning social scoring or facial recognition merely to prevent abuse of fundamental rights by public authorities reveals a less than holistic view of their social consequences in private companies. The same technologies are in fact meticulously applied in workplaces to recruit, evaluate, and dismiss with equally relevant social impacts on the fundamental rights of European citizens and workers. Their missing prohibition in employment contexts, again, has been avoided for the usual fear of holding back technological development in the private sector [25]. When particular uses of AI, such as scanning candidates’ interviews or CVs, are increasingly proven to be discriminatory against minorities [26].

The proposed AI Act is not a satisfactory proposal. Yet it raises an important dualism for the future of labour regulation. Data governance and technology governance are two different things. While in the coming years it will be possible to rethink data protection according to the social externalities of data science, today these two governances can be complemented, with interesting results under a labour regulation perspective. Such complementarity might curb the social impact of new technologies in specific applications. Thus, enacting a government of data and a government of digital technologies, for a sustainable digital development as sought by the EU Commission Industry 5.0 strategy towards the ‘sustainable, human-centric and resilient European industry’ [27]. Technology governance, which, moreover, has in the history of labour law played a

major role in restricting new technologies to protect the health and safety of the workforce [28]. The dual track of data and technology governance thus might overcome the strongest assumption of these days: that market-driven innovation in workplaces can be effectively channelled by existing data protection standards to protect workers' rights. Therefore, letting a legal assessment of technologies' social impact be introduced in our European and national legislations [29].

Concluding with a case and a provocation: there is sufficient evidence of bias and strong discrimination by software that analyses CVs or scans faces at job interviews to infer personal information about candidates. Today, in the debate around the AI act, would it still be a Luddite idea to ban their uses (as it is already proposed for social scoring and facial recognition in public places)?

---

## References

- [1] The New York Times, 14 August 2022, The Rise of the Worker Productivity Score, <https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html>; See also De Stefano, Valerio and Wouters, Mathias, AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework (March 1, 2022). Osgoode Legal Studies Research Paper Forthcoming, Available at SSRN: <https://ssrn.com/abstract=4144899>
- [2] Jarrahi, Mohammad Hossein, et al. (2021), "Algorithmic Management in a Work Context." *Big Data & Society*, July 2021, doi.org/10.1177/20539517211020332
- [3] Molè, Michele (2022), The Quest For Effective Fundamental Labour Rights in The European Post-Pandemic Scenario: Introducing Principles of Explainability and Understanding For Surveillance Through AI Algorithms and IoT Devices (May 1, 2022). 19th International Conference in Commemoration of Marco Biagi "Work Beyond the Pandemic. Towards a Human-Centred Recovery", 2022, Available at SSRN: <https://ssrn.com/abstract=4099663> or <http://dx.doi.org/10.2139/ssrn.4099663>
- [4] European Commission, Directorate-General for Research and Innovation, Renda, A., Schwaag Serger, S., Tataj, D., et al., *Industry 5.0, a transformative vision for Europe: governing systemic transformations towards a sustainable industry*, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2777/17322>
- [5] Risak, Martin and Dullinger, Thomas (2018), The Concept of 'Worker' in EU Law: Status Quo and Potential for Change (June 5, 2018). ETUI Research Paper – Report 140, 35, Available at SSRN: <https://ssrn.com/abstract=3190912> or <http://dx.doi.org/10.2139/ssrn.3190912>
- [6] Ball, Kristie (2010), Workplace surveillance: an overview, *Labor History*, 51:1, 89, doi.org/10.1080/00236561003654776
- [7] Ibid, 88.
- [8] Hiranandani, Vanmala (2011), 'Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions' 15 *The International Journal of Human Rights* 1091, 1092 <<http://www.tandfonline.com/doi/abs/10.1080/13642987.2010.493360>>

[9] Niemietz v Germany: ECHR 16 Dec 1992, para 29, <https://hudoc.echr.coe.int/eng?i=001-57887>

[10] Kim, Pauline and Bodie, Matthew T. (2021), Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy (September 2021). 35 ABA Journal of Labor and Employment Law 289 (2021), Washington University in St. Louis Legal Studies Research Paper No. 21-09-02, Saint Louis U. Legal Studies Research Paper No. 2021-26, Available at SSRN: <https://ssrn.com/abstract=3929066>

[11] Kaminski, Margot E (2018)., The Right to Explanation, Explained (June 15, 2018). U of Colorado Law Legal Studies Research Paper No. 18-24, Berkeley Technology Law Journal, Vol. 34, No. 1, 2019, Available at SSRN: <https://ssrn.com/abstract=3196985> or <http://dx.doi.org/10.2139/ssrn.3196985>

[12] See Molè, n. 3, 6-11.

[13] Otto, Marta (2016), The Right to Privacy in Employment: A Comparative Analysis, 194

[14] Viljoen, Salome (2020), A Relational Theory of Data Governance (November 11, 2020). Yale Law Journal, Forthcoming, page 7 and 48 Available at SSRN: <https://ssrn.com/abstract=3727562> or <http://dx.doi.org/10.2139/ssrn.3727562>

[15] Ibid, pp. 41-52

[16] Article 9 of the GDPR provides for the prohibition of the collection and processing of sensitive data (racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, health or data concerning a natural person's sex life or sexual orientation), however, if the employer collects explicit consent from the employee or it is necessary for the performance of the [employment] contract, such data would be usable; de facto an empty rule.

[17] Otto (2016), 194-195

[18] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts Com/2021/206 Final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

[19] See European Commission, n. 4.

[20] See n. 18, art. 6 (2) and Annex III.

[21] Otto (2016), 185, 194-195. See also Negrón, Wilneida (2021) 'Little Tech Is Coming for Workers. A Framework for Reclaiming and Building Worker Power.' (CoWorker.org 2021) <<https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf>>

[22] Halefom H Abraha (2022), A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace, International Data Privacy Law, <https://doi-org.proxy-ub.rug.nl/10.1093/idpl/ipac015>

[23] Ponce Del Castillo, Aida (2021), The AI Regulation: entering an AI regulatory winter?, ETUI

---

Policy Brief, 2021/07,  
<https://www.etui.org/publications/ai-regulation-entering-ai-regulatory-winter>

[24] De Stefano, Valerio (2021), The EU Proposed Regulation on AI: a threat to labour protection?,

<http://global-workplace-law-and-policy.kluwerlawonline.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/>

[25] Ramos Alvarez, Mauricio (1999) 'Modern Technology and Technological Determinism: The Empire Strikes Again' (1999) 19 Bulletin of Science, Technology & Society 403 <<http://journals.sagepub.com/doi/10.1177/027046769901900508>> accessed 22 May 2022.

[26] Kim and Bodie (2021)

[27] See European Commission, n. 4.

[28] European Agency for Safety and Health at Work (2022), Artificial intelligence for worker management: implications for occupational safety and health, <https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-implications-occupational-safety-and-health>

[29] Ramos Alvarez (1999). See also: Lauren E. Elrick (2021) The ecosystem concept: a holistic approach to privacy protection, International Review of Law, Computers & Technology, 35:1, 44-45, DOI: [10.1080/13600869.2020.1784564](https://doi.org/10.1080/13600869.2020.1784564)

This entry was posted on Wednesday, November 23rd, 2022 at 8:00 am and is filed under [Data protection](#), [EU Law](#), [Labour law](#), [Privacy](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.