From Digital Vulnerability to Data Anxiety: The Situation of Employees in Digitally Permeated Workplaces

Isabelle Wildhaber, Isabel Laura Ebert

A. Introduction

People may perceive digital data with a sense of fear or «data anxiety» regarding data security, surveillance practices or power relationships. Such anxieties demonstrate how «digital data is rarely thought of by its everyday users as safe, easy to access or manage, or, in the case of personal data, necessarily accurate.»[1] In that sense, digital vulnerability can be seen as a useful concept to capture the fluid and multilayered nature of the human condition when opposed to digitally permeated spaces. Digital vulnerability as a conceptual basis allows us to question the adequacy of some foundational legal and policy norms regarding the situations of employees in digitally permeated workplaces.

This chapter contributes to identifying the factual conditions in which digital technologies might prove disruptive and challenging for people in workplace settings, and in assessing under which conditions, how and to what extent the notion of digital vulnerability might be translated into claims for special legal protection at work. Employees have always been vulnerable in their contractual relationship with their employers, which is why in most countries the employment contract is heavily regulated[2] and contractual autonomy is limited in employment contracts to compensate the perceived inequality of the two contractual parties. In times of digitally permeated workplaces, the vulnerability of employees increases as they become subject to monitoring and control practices by digital technologies.[3]

1 Sarah Pink, Debora Lanzeni and Heather Horst, 'Data anxieties: Finding trust in everyday digital mess' (2018) 5 Big Data & Society 1.

2 Brishen Rogers, 'Workplace Data and Workplace Democracy' (2022) 6 Geo L Tech Rev 454.

3 Isabel Laura Ebert and Isabelle Wildhaber, 'Privacy in the Workplace: A Human Rights Due Diligence Approach' in Jonathan Andrew and Frédéric Bernard (eds), *Human Rights Responsibilities in the Digital Age: States, Companies and Individuals* (Oxford Hart Publishing 2021).

Employees can barely structurally resist or circumvent being subject to digital monitoring or control. Digital vulnerability of employees makes it necessary to reflect upon future changes to national employment laws and to corporate due diligence processes to protect employees from the exposure to harm that might arise from interaction with digital technologies and to address employees' digital vulnerability.

Digital vulnerability is entering into employment relationships via new, data-based forms of algorithmic management. Algorithmic management tools collect data about employees in large and granular quantities to evaluate them in real time or at high speed with the help of algorithms. This results in correlations and metrics on myriad variables about the individual employee.[4] Components of workers' social and organizational lives are transposed into numerical data by technologies with the aim to increase efficiency.[5] Depending on the contextual set-up, there is a high risk that algorithmic management may constitute a new form of surveillance, increasing the digital vulnerability of employees.[6]

Algorithmic management systems combine traditional employment data (e.g., performance appraisals, sick days, or salaries) and new data (e.g., social media activity logs, sensor data, consumer data from GPS or tracking systems) to create processes for identifying, recruiting, retaining, and rewarding job candidates as well as employees. They promise to optimize operations, increase efficiency and innovation, the improvement of employee satisfaction, the reduction of prejudices in decision-making processes, or more objectivity and diversity within the company.[7]

Algorithmic management systems are applied in a range of areas, such as employee selection/recruitment, performance management, compliance management, employee retention and development, work and workplace

4 Isabelle Wildhaber, Melinda Florina Lohmann and Gabriel Kasper, 'Diskriminierung durch Algorithmen–Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz' (2019) Zeitschrift für Schweizerisches Recht I 459, 461 ff.

5 Kenneth Cukier and Viktor Mayer-Schoenberger, 'The rise of big data: How it's changing the way we think about the world' (2013) 92 Foreign Aff 28.

6 Isabel Ebert, Isabelle Wildhaber and Jeremias Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection' (2021) 8 Big Data & Society 1.

7 Ifeoma Ajunwa, Kate Crawford and Jason Schultz, 'Limitless worker surveillance' (2017) California Law Review 735, 743; Roger W Reinsch and Sonia Goltz, 'Big Data: Can the attempt to be more discriminating be more discriminatory instead' (2016) 61 Louis ULJ 35, 46; Rebecca J Wilson, Kiley M Belliveau and Leigh Ellen Gray, 'Busting the black box: Big data, employment and privacy' (2017) 84 Def Counsel J 1, 32.

design.[8] While electronic employee surveillance has been criticized by scholars since decades, algorithmic surveillance as a modern form of employee surveillance differs from traditional electronic surveillance in the workplace by three factors: (1) variety of data, (2) interoperability between systems, (3) increasing analytical performance of the systems.[9] These factors contribute to the increase of digital vulnerability of employees. As a result, employers now enjoy near-plenary powers to monitor and control workers in the worksite and often during non-work hours as well.

In this chapter, we refer to algorithmic management systems or to «Automated Decision-Making Systems», in short ADM systems.[10] ADM systems are used to predict, recommend, influence, or decide about humans. In most systems, a human still monitors, overrides or decides (decision-support systems with a "human in the loop" and only partial automation).[11] However, qualitative empirical evidence from our recent research project shows that people generally adhere to the suggestions of an algorithmic management system and only occasionally and with reluctance actively reject and override these suggestions.[12] This shows that it does not matter whether we deal with a system that is decision-making (in the sense of art.

8 Isabelle Wildhaber and Gabriel Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz' in Roland A. Müller and others (eds), *Festschrift für Wolfgang Portmann* (Schulthess 2020), 759; Gabriel Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts', (Universität St. Gallen 2021), 42 ff.

9 Wildhaber, Lohmann and Kasper, 'Diskriminierung durch Algorithmen–Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz', 463; Wildhaber and Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz', 758 ff.; Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, 71 ff.; Kirstie Ball, 'Workplace surveillance: An overview' (2010) 51 Labor History 87.

10 European Law Institute, 'Guiding Principles for Automated Decision-Making in the EU' (2022) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf> accessed 26 October 2023, 8.

11 algo:aware, 'State-of-the-Art Report | Algorithmic decision-making' (2018) <https://actuary.eu/wp-content/uploads/2019/02/AlgoAware-State-of-the-Art-Report.pdf> accessed 26 October 2023, 7 and 11; Jeremias Adams-Prassl and others, 'Regulating algorithmic management: A blueprint' (2023) 14 European Labour Law Journal 124, 20 ff.

12 Isabelle Wildhaber and Isabel Ebert, 'Piercing the Veil of Opacity: Responsibility and Liability for People Analytics Tools at the Workplace' (2022) 1 Morals & Machines 40.

22 GDPR) or one that is only decision-suggesting, in both cases there is significant impact on the employees affected.

In order to portray empirical insights about workplace practices around digital technologies and its impact on employees, this chapter depicts quantitative data about the uptake of algorithmic management tools in Switzerland, as well as a deep dive into qualitative data from case studies that demonstrate the interactions of employees, their supervisors and digital technologies at the workplace, and how it impacts employee perceptions of digital vulnerability (B.). Building on empirical evidence, the chapter sketches several avenues for solutions, both on the legal level through the strengthening of collective worker representation and grievance mechanisms (C. and D.). The chapter also addresses key ethical aspects and proposes better processes to uphold duty of care towards employee well-being at the company level (E.). By showing empirical insights into impacts of current digital workplace monitoring practice on employee vulnerability, this chapter aims at contributing to identify how to reduce digital vulnerability of employees in digitally permeated workplaces.

B. Empirical insights about employee vulnerability in digitally permeated workplaces

This chapter builds on insights gathered as part of our research project «Big Brother in Swiss companies? Trust, data and privacy at work», funded by the Swiss National Science Foundation from 2017 to 2021.[13] The data consists of an empirical quantitative survey from a Switzerland-wide survey on the use of ADM systems in the workplace (2018, 2020), as well as five qualitative case studies in big Swiss corporations (2020, 2021). For reasons of confidentiality, the data is only presented in aggregated and anonymous form. We have specifically processed and reviewed our empirical data for the purpose of emphasizing the aspects of digital vulnerability found in it.

13 <https://www.nfp75.ch/de/rWt7Xm4jTGt4imB7/projekt/projekt-weibel> accessed 26 October 2023.

I. Results from a quantitative survey in Swiss companies

The results of the Switzerland-wide quantitative survey, primarily aimed at those responsible in human resources (HR) departments, are described in the following. In 2018, we conducted an online survey in which 158 large Swiss companies took part, in which these companies were asked whether they use certain IT-based tools for algorithmic people management.[14] 35.4% of participants reported not using any of these tools, while 64.6% used such tools. The online survey was repeated in 2020.

The results of the comparison of the first survey in 2018 and the repeat survey in 2020 showed the current maturity of datafication in the Swiss workplace. The biggest trend comparing the 2018 survey to the 2020 survey was an 18% increase in *Hiring & Recruiting* tools. The 2020 survey found that 39% of Swiss companies included in the survey use partially automated analytics tools to make an initial selection among applicants. Sometimes a tool is used to manage the recruiting process (e.g., reminder of applicant waiting time, automatic conversation). For applicants, in very few cases psychological tests are combined with pattern and speech recognition in applicant files. Algorithmic management tools are most widespread in the area of *Retention & Transition* (63% in 2020), with an increase of 2% compared to the first survey in 2018. Algorithmic management tools with less complex algorithms are used most often. More complex algorithms are mainly used for further processing of analogously collected employee data, for example in the context of linking in HR dashboards. Many low-tech versions of online surveys are used, sometimes as pulse surveys and even more rarely as employee experience dashboards. *Performance Management* tools are in second place (47% in 2020), up 10% from 2018. For example, automated tools for tracking keystrokes and internet usage are widespread, and some companies have begun to use time analysis tools. In terms of *Compliance Management* and *Work & Workplace Design*, there were no major changes between the 2018 and 2020 surveys: Compliance Management saw only a slight overall increase of 4% to 22% in 2020; Work & Workplace Design saw an overall decrease of 2% to 36% in 2020.

It is interesting to note that the 2018 quantitative survey also revealed that most companies do not involve external stakeholders in the design and use of algorithmic management tools. Only 5% of respondents involved busi-

14 Wildhaber and Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz', 764 ff.

ness associations, 8.8% involved business owners, 10.5% involved unions, 28% involved academics, and no companies reported working with civil society. Peer-to-peer exchanges (50.9%) and involvement of consulting firms (59.6%) were the most prominent external stakeholders involved in the design and use of algorithmic management tools. In general, apart from peer-to-peer and consulting companies, there is little exchange with external stakeholders, so that independent expert knowledge is only used by a few companies. Hence, external expertise on creating a workplace for employee well-being and for reduction of digital vulnerabilities is not structurally taken into consideration.

II. Results from the five qualitative case studies in Swiss multinational companies

In the context of the already sketched quantitative developments around the use of workplace monitoring technologies in Swiss companies, the qualitative empirical analysis, as presented in the following, can provide additional insights into aspects of digital vulnerability of employees at the workplace.

The qualitative case studies were carried out in five large Swiss corporations with 20-25 employees and managers between 2018 and 2020. The expert interviews were conducted with employees as well as managers and business strategists. In analyzing the qualitative data for this chapter on digital vulnerability, the focus was on the question of how employees are involved in the design of ADM systems, how they can voice concerns and whether such concerns are taken into consideration, and how this relates to the more general processes for introducing and developing ADM systems. We analyzed the interviews with broad thematic coding.[15] The results are presented below.

To provide more context, in our qualitative case studies, ADM systems were used to plan routes in the logistics industry and to monitor driving behavior in terms of compliance with road traffic regulations and as an incentive to save fuel. Other examples of use in service companies were ADM systems for career planning and identification of talents in the internal personnel pool, or work process-accompanying ADM systems for customer management or claims processing in the insurance industry.

15 Matthew B Miles and A Michael Huberman, *Qualitative data analysis: An expanded sourcebook* (Sage Publications 1994).

1. Information

In some companies, interviewees reported that information about ADM systems could be found on the intranet, but that the introduction of ADM systems was not actively accompanied by a communication process. Therefore, many employees felt poorly informed or did not know exactly what the ADM systems measured at what time and in what way, and what decisions were made on the basis of these measurements or later analyses based on the measured values.

In other companies, a pilot project was launched before the official introduction of the ADM systems. Within this pilot project, companies created an informal mechanism for employee representation. The pilot teams worked, among other things, with so-called power users who came from the workforce and were supposed to educate the teams about the digital technologies that were being used. These power user employees acted as a point of contact for potential suggestions for improvement, praise, criticism, and complaints from the workforce regarding the implementation of the ADM system. However, it was often not obvious to what extent and in what way these insights from the pilot projects influenced the later, organization-wide implementation. The process as such could not claim to be a formal process under labour law.

Other companies launched large-scale culture campaigns on the handling of data in general, and widely distributed information on algorithmic management tools in particular. Many employees perceived this as positive and as creating transparency and making them feel less vulnerable. As a result, employees were on average better informed than in companies where only non-targeted information was available on the intranet without being actively communicated.

Particularly in the introductory phases of the technology, many employees often felt caught off guard or there were methodological problems, i.e., the metrics that were supposed to be recorded were not really collected in a targeted manner. In part, newer technical versions therefore brought better acceptance, but even these «teething troubles» could not be fully addressed, and employees felt digitally vulnerable and punished for technological bias and/or inaccuracy.

2. Consultation

In our case studies, the way in which information was provided affected employees' potential for consultation and for reducing their digital vulnerability by voicing concerns or asking for adaptations. Additionally, if employees had fundamental problems understanding data processing and the scope of ADM systems, they could not participate in consultation processes in an informed manner.

In certain companies, one individual (power user) acted as a kind of guiding figure and contact person for the implementation of ADM systems, but no formalized process for complaints or suggestions or criticism existed. Feedback loops regarding complaints or concerns were very rarely mentioned or described. The fact that feedback during the introduction process is carried out in some companies through informal channels makes the consultation process very informal («casualization»). At the same time, informal feedback cultures could lower the perceived threshold for giving genuine feedback. Such informal processes are far removed from participation respectively information and consultation in the labour law sense. Communication along successive introductions of beta versions and a start-up mentality cannot replace a more formal collective participation mechanism for making employee voices heard. In addition, consultations at the collective level were extremely rare, although they would be more appropriate to the systematic nature of the widespread use of ADM systems.

A participation possibility was mostly made possible either through pilot projects, or through the individual contact of employees via the respective manager. Some companies have introduced employee participation in pilot projects: For instance, one manager explained that «*employees are involved early on when it comes to various, or all, issues that affect employees. We have a very active exchange. It starts with the planning of structural changes, the conversion of fixed workstations to open-plan offices with shared use, and so on. Employees are always involved in issues at an early stage*». This is an example of how pilot projects can be designed and implemented with employee participation, and for ensuring employees can express concerns about set-ups/situations that are digitally mediated and make them feel vulnerable. However, these processes cannot fully substitute for formal collective participation for scaling the use of ADM systems after the pilot phase is complete, as they can never reflect the diversity of the entire workforce's day-to-day work.

3. Data protection law as a buffer against the inappropriate use of ADM systems

For some ADM systems, data protection law did not permit data collection, and/or processing in specific use cases. As a result, sometimes, data protection law functioned as employee protection. This includes applications of ADM for which the purpose-specific data requirement is not met, because personal data is used for several purposes. Here, not only the prior information/consent of the data subject was missing, but there was also a lack of the necessary purpose limitation.

However, data protection law should not be the only method to strengthen protection as the possibilities for objection in data protection are individual in nature and not collective, hence collective effects at scale for reducing employee vulnerability are minimal.

4. Attribution of responsibility and exercise of power

In many scenarios, ADM systems reinforce the hierarchical power asymmetry between supervisors and employees.[16] In addition, qualitative empirical evidence from our research project shows a mismatch in the attribution of responsibility with respect to ADM-based decisions. From the employees' point of view, a clear responsibility is attributed to the supervisor («*clearly the boss is responsible for this*»). At the same time, from the supervisor's point of view, the responsibility is predominantly shifted away to «the machine» («*I can't do anything about it, it was technically determined*»). This can lead to a diffusion of responsibility, which is very problematic in this power constellation and this dependency relationship regarding performance evaluation, and the heightened digital vulnerability of employees.[17] Our empirical findings confirm the discussion in the literature and suggest that ADM systems reinforce the power imbalance between managers and employees.[18]

16 Katherine C Kellogg, Melissa A Valentine and Angele Christin, 'Algorithms at work: The new contested terrain of control' (2020) 14 Academy of Management Annals 366.

17 Simon Schafheitle and others, 'The Bermuda Triangle of Leadership in the AI Era? Emerging Trust Implications from Two-Leader-Situations in the Eyes of Employees' (2020) in HICSS.

18 Will Sutherland and others, 'Algorithmic management in a work context' (2021) 8 Big Data and Society.

5. Communication as a means to engage employees

Some companies have implemented several internal communication tools to improve employee awareness and digital literacy across all departments. One employee explained: «*I think that's also a communication problem when you just say 'this and this is the goal' and you don't address their (employees') fears, you just let it simmer a little bit. Then the rumors start like 'this is automation'*.» Ideally, both employers/supervisors and employees are on the same page when it comes to understanding the core objectives of using ADM systems, which can contribute to the development of a common understanding within the organization and reduce perceptions of digital vulnerability on the sides of the employees. As described earlier, this was not the case in all companies: instead, some companies relied on uploading documents to the intranet without a corresponding accompanying information campaign to raise awareness across the workforce.

6. Learning culture vs. sanctioning culture

Our interviews revealed that the way in which digital technologies are implemented and managed in workplace monitoring plays a key role in whether ADM systems become an empowering tool or whether a culture of sanctioning emerges as result of digital technology use. Workers interviewed offered insights into the sometimes unrealistic expectations assigned to the capacity of digital technology, which measures the exact time it takes a worker to complete their activity, such as delivering goods, and does not take into account other factors that might affect time (e.g., weather or traffic). For example, interviewed workers reported that supervisors ask their workers, «*What have you done in these 8 minutes? It is 30 meters from this house to that house, it should take 30 seconds.*» Employees reported that some measurements were also inaccurate, e.g., the technology did not account for a reduction in speed when road conditions were snowy and icy. Despite inaccurate results, disciplinary action was sometimes taken against employees. In such cases, the technology punishes employees instead of empowering them to work more efficiently or safely/carefully.

The ability to contextualize technical measurements was not necessarily a given in most of the companies surveyed, and in some cases was patchy. Nevertheless, some companies were making efforts to improve the culture to link technology to a learning culture, with so-called data culture initiatives or data culture boards. Supervisors that had an increased level of

awareness of the need to contextualize technology use paid attention to the level of inference, for example, saying «*We want a culture of error, not a command tone, we want people to learn from their mistakes - we don't want people to feel exposed*».

In the companies that invested heavily in establishing an «error culture», supervisors and employees viewed the metrics from the ADM systems primarily as a basis for discussion in their regular performance evaluations and felt less vulnerable to be punished for technological shortcomings. Other companies, on the other hand, considered the readings to be irrevocable and took negative consequences for employees for non-compliance, even if the accuracy of the technological track record was poor, e.g., penalizing them for driving too slowly and using low gears when driving on icy, snowy roads, even if that was the responsible behavior in that very situation.

7. Acceptance of ADM systems

The acceptance of the use of technology by the employees was promoted by the learning culture, the possibility of participation, as well as careful information and communication that was prepared in a way that was appropriate for the target group. The acceptance is also an opportunity to increase the effectiveness of the use of ADM systems, for example, since, according to our studies, a low level of acceptance led to tricking by employees and thus negatively influenced the measurement quality, i.e. the data input often no longer represented the measurement value that was originally intended to be collected.

C. National and international legal foundations

I. National legal foundations

In national laws, there are commonly several applicable regulations that usually apply to the use of ADM systems: Data protection law, employment law, health and safety regulations, privacy protection, employee participation and discrimination protection.[19] Our empirical quantitative studies have shown that many prerequisites of national laws are not fulfilled in

19 Ebert, Wildhaber and Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection'.

practice. Also, legal greyzones exist when it comes to employees' rights where ADM systems are being used. Furthermore, there are many regulatory gaps due to information asymmetries, increase in privacy harms, algorithmic discrimination, or lack of human agency.

Illustratively, in the context to our empirical data, according to Swiss employment law (art. 328b Code of Obligation) the processing of personal data at the workplace requires that the data is workplace-related. However, our research showed that 3% of employers collect non-occupational data from their employees and 7% of employers collect non-occupational data from their job applicants.[20] According to Swiss workplace health and safety regulations (art. 26 Ordinance 3 to the Labour Act) surveillance systems to control employee behaviour are prohibited. However, 22% of all employers do observe employee behaviour.[21]

Adding to this, according to the Swiss Federal Act on Data Protection (art. 19), the collection of personal data and the aim of the collection has to be transparent to the concerned person. However, only 53% of employees understand which input the employer analyzes.[22] The required employee consent must be informed (specific and adequate) and voluntary (art. 6 and 7). Our quantitative empirical studies have shown that 59% of employers ask for a general consent in the employment contract, 27% of employers ask for a specific consent for each use of a tool, 11% do not ask for consent.[23] Therefore, some ADM applications we analyzed were outside the scope of the applicable law.

And finally, according to the Swiss Participation Act (art. 10 lit. a) collective participation is often necessary for the introduction and implementation of algorithmic management tools. Yet, this is not happening in practice: Employee representations and trade unions are only involved as external stakeholders in the design and use of ADM systems in 10.5% of cases.[24]

Summing up, the use of digital technologies at the workplace in Switzerland is currently not fully guided by the legal foundations and some companies seem to be consciously or non-intentionally taking legal risks, as well as implementing ethically questionable practices.

20 Wildhaber and Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz', 767.
21 ibid, 768.
22 ibid, 769.
23 ibid, 769.
24 ibid, 770.

II. International legal foundations

Regarding workplace law issues, national legal foundations are predominant. Labour law and employment law traditionally belongs to the regulatory sovereignty of the state concerned. Across Europe, however, with respect to data protection issues, EU data protection law, in particular the GDPR, as well as national laws of the member states (art. 88 GDPR) should be consulted.[25] Equally, for the European context and related to data protection, Convention 108 of the Council of Europe is relevant. Convention 108 is the first binding but not directly applicable treaty on data protection.[26] The Convention aims to protect the right to privacy in the automatic processing of personal data (art. 1 Convention 108). To this end, the Convention provides a set of data protection principles, as well as instructions for cooperation between the Parties in the implementation of the Convention. The Convention applies to automated data collections and files and to automated processing of personal data in both the public and private sectors (art. 3 para. 1 Convention 108).[27]

Globally, the protection of privacy rights between private individuals is protected by the International Covenant on Civil and Political Rights (UN Covenant II). Art. 17 protects against arbitrary or unlawful interference with private life, family, home or correspondence, as well as against unlawful impairment of honor or reputation.[28] With regard to the participation rights of employees, a wide variety of provisions of international law must be considered. For example, the European Convention on Human Rights (ECHR) must be taken into account. Art. 8 European Convention on Human Rights (ECHR) establishes a human right to respect for private and family life. According to the case law of the European Court of Human

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 (2016); Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, 109ff.

26 Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'CETS No. 108' (1981).

27 Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, 130.

28 United Nations, International Covenant on Civil and Political Rights (ICCPR) (1976).

Rights (ECtHR), the term private life can also include professional activities.[29]

The protection of the employee health is an obligation under international and constitutional law. These obligations are anchored, in particular, in art. 6-8 (right to healthy and safe working conditions) of the International Covenant on Economic, Social and Cultural Rights (ICCPR or UN Covenant I). In June 2022, health and safety at work was declared a fundamental principle of the International Labor Organization (ILO).[30] The basic principles of the ILO were developed in ten conventions. The recognition of health protection as a further fundamental principle means that ILO Conventions 155 and 187 now have the status of core labour standards and thus of universally valid human rights.[31] They thus constitute a minimum standard below which all ILO member states may not fall. With ILO Convention 155, the member states undertake to pursue a national policy of preventing accidents and damage to health that occur as a result of or in connection with work (art. 4 para. 2 ILO 155). The more recent ILO Convention 187 supplements the provisions of ILO Convention 155 and aims to specify the implementation of the prevention of accidents or damage to health in the context of work.

In the Community law of the European Union, great importance is attached to the protection of the health of employees. This is reflected in the recitals of Council Directive 89/391 of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers. The Organisation for Economic Co-operation and Development (OECD) has also published a number of principles that are relevant to the use of ADM systems. The OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD MNE Guidelines) stipulate, for example, an anti-discrimination requirement, according to which companies should be guided by the principle of equal opportunities and equal treatment in the activity of employing workers. Furthermore, section V para. 3 of the OECD Guidelines stipulates a duty of consultation and

29 BĂRBULESCU v. ROMANIA App no 61496/08 (ECHR), Recital 71.

30 International Labour Organization, 'A safe and healthy working environment is a fundamental principle and right at work' 2022) <https://www.ilo.org/global/topics/safety-and-health-at-work/areasofwork/fundamental-principle/lang--en/index.htm> accessed 26 October 2023.

31 International Labour Organization, 'ILO Declarations' <https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/organigramme/jur/legal-instruments/WCMS_428589/lang--en/index.htm> accessed 26 October 2023.

cooperation on the part of the employer vis-à-vis the employees or their representatives in «matters of common interest».[32] The UN Guiding Principles on Business and Human Rights (UNGPs), discussed in the following, are consistent with the OECD Guidelines. In addition, the OECD has published recommendations on the use of artificial intelligence in 2022. In these, the OECD points out that the use of AI in companies must, among other things, respect internationally recognized employee rights, data protection and anti-discrimination.[33] In a similar vein, the UNGPs encompass the technology sector. Broadly speaking, the Business & Human Rights framework is centered around the UNGPs. The Business & Human Rights Framework outlines the State duty to protect against human rights abuses stemming from or being linked to company activities, and businesses' responsibility to respect human rights, and to provide remedies for individuals who have been harmed by business activities.[34] The UNGPs consist of 31 guiding principles, which are structured into three pillars that provide a framework for governments and businesses to protect and respect human rights. The three pillars are: (1.) the State duty to protect human rights, (2.) the corporate responsibility to respect human rights, and (3.) access to remedy. The UNGPs provide a framework for businesses to identify, prevent, mitigate, and remedy human rights impacts associated with their operations, products, and services, and are widely recognised as the authoritative international standard for responsible business conduct, along with the OECD MNE Guidelines.

The central concept of this corporate responsibility towards people and their rights is the company's human rights due diligence, which is based on the logic of operational risk management processes, but specifically on risks to people, and thus also on the rights of employees. The UNGPs are frequently referenced in corporate policies and processes because they are based on the universally recognized framework of human rights and enshrine the "minimum standard for responsible behavior" by private companies. The UNGPs are implemented by a large number of global

32 OECD, 'OECD Guidelines for Multinational Enterprises on Responsible Business Conduct' <https://www.oecd-ilibrary.org/content/publication/81f92357-en> accessed 26 October 2023.

33 OECD, 'Recommendation of the Council on Artificial Intelligence' <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 26 October 2023.

34 OHCHR, 'Guiding Principles on Business and Human Rights' (*United Nations,* 2011) <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 26 October 2023.

corporations and are increasingly reflected in national legislation and national policy packages. Switzerland has also committed to implementing the UNGPs, including within the framework of a National Action Plan for Business and Human Rights. France passed the "loi de vigilance" (Duty of Care Act) in 2017, and in Germany the Supply Chain Due Diligence Act came into force on January 1, 2023. On 25 July 2024, the European Union adopted a directive on corporate sustainability due diligence (Directive 2024/1760), that also builds on the UNGPs.

There is, of course, also the possibility of dealing with adverse impacts on human rights being linked or stemming from business activities through non-legal means in the form of the mediation processes of the so-called National Contact Point for Responsible Business Conduct of the OECD, which can be found in each member state of the OECD.

Context-specific ethical approaches, e.g. for the context of digital technologies at the workplace, can be combined with the UNGPs insofar as the UNGPs show the minimum standard that can be expected and take contextual factors into account when exercising the duty of care. These due diligence obligations are therefore obligations to establish certain systems and processes in companies in order to identify, address and mitigate adverse impacts on human rights, and to help those affected in the event of complicity or involvement in human rights abuses.

The UNGPs stipulate that companies establish processes through which they identify and address human rights risks and through which they take measures to reduce or, ideally, eliminate these risks. Broadly speaking, the human rights due diligence process can be divided into four steps[35]:

a. Identify and assess the impact of business activities on human rights in order to assess the nature and extent of human rights risks;
b. Act to prevent and mitigate human rights risks, including through integration into internal functions and processes;
c. Track the effectiveness of risk mitigation measures over time;
d. Adequate communication of measures to address human rights impacts.

Structuring the due diligence responsibilities along the UNGPs is helpful for implementation in the company when using ADM systems in the work-

35 B-Tech, 'Key Characteristics of Business Respect for Human Rights' (*United Nations Human Rights Office of the High Commissioner,* 2020) <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/key-characteristics-business-respect.pdf> accessed 26 October 2023.

place. The human rights affected may include the right to privacy, the right to non-discrimination or the right to health. However, the UNGPs recommend an analysis in relation to all human rights and a prioritization of measures based on the possible severity of a human rights impact («severity»).[36] Human rights due diligence will look different in various organizations and contexts. However, certain features of human rights due diligence are particularly important when addressing human rights risks related to technology products, services and solutions.

The UNGPs have established themselves as a global standard for corporate responsibility and are used by many large technology companies, which is evident, among other things, based on publicly available risk analyzes and reports. For example, the multi-stakeholder organization Global Network Initiative regularly reviews the implementation of the UNGPs in its member companies.[37] Employees affected by companies headquartered in an OECD member state can initiate mediation proceedings at the respective National Contact Point for Multinational Companies.

Lastly, consider the UN Sustainable Development Goals (SDGs). The eighth goal is dedicated to promoting inclusive and sustainable economic growth, employment and decent work for all. The eighth goal is divided into 12 sub-categories - Goal 8.8 reads, «Protect labour rights and promote safe and secure working environments for all workers, including migrant workers, in particular women migrants, and those in precarious employment».[38]

36 B-Tech, 'Taking Action to Address Human Rights Risks Related to End-Use' (*United Nations Human Rights Office of the High Commissioner,* 2020) <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/taking-action-address-human-rights-risks.pdf> accessed 26 October 2023.

37 Global Network Initiative, 'Company Assessments' <https://globalnetworkinitiative.org/company-assessments/> accessed 26 October 2023.

38 United Nations Department of Economic and Social Affairs, 'Goal 8: Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all' 2015) <https://sdgs.un.org/goals/goal8> accessed 26 October 2023.

D. Suggestions to address regulatory gaps in digital vulnerability of employees

The majority of ADM systems are operated with a human still monitoring and possibly overriding the ADM system (human in the loop).[39]. At the same time, our qualitative case studies showed that humans usually stick to the suggestions of the ADM system, and only actively reject and override these suggestions sporadically and with restraint. In fact, most employees followed the ADM-based suggestions, so it is very likely that human decision-making was predetermined. A "human in the loop" is therefore not enough to ensure that the output of an ADM system has significant negative effects on the people about whom the decision is made and that a human assessment of the facts actually takes place.

I. Strengthening collective participation

Employees are the main "data providers" of ADM systems at the workplace. One of the main tasks of employees and their representatives is to create a counterweight to the prerogatives of employers and to address collective risks and damages within the framework of social dialogue. Strengthening the rights of employees, their representatives and unions is therefore an evident option. The employer must be obliged to inform its employees not only individually (as in data protection laws) about ADM systems, but also collectively. Collective participation rights must exist in the development, procurement, configuration and use of ADM systems as well as in all changes to the ADM system or its configuration that affect, or are likely to affect, working conditions. Furthermore, ADM systems must become an important topic of social partnerships.

This could be accomplished as follows, whereby the suggestions listed here are to be understood as a possible sample of options and as non-exhaustive:

1. Given the complexity and opacity of ADM systems, employee representatives can only fulfill their tasks if they receive transparent, precise, understandable, relevant and timely information about the planned deploy-

39 Wildhaber and Ebert, 'Piercing the Veil of Opacity: Responsibility and Liability for People Analytics Tools at the Workplace', 43; Adams-Prassl and others, 'Regulating algorithmic management: A blueprint', 20ff.

ment, intended use, expected impacts and operation of ADM systems. This also serves transparency. The employee representatives need information about the actors involved (developers, implementing positions within the company) and about any impact assessments, potential risks and planned risk minimization measures. It is important that all information is communicated in a format that is understandable, comprehensible and appropriate to the expertise of the recipient. To ensure that the information does not become too long to absorb for the individual or is overloaded with "meaningless" information, the legislature could set requirements for the type, clarity and scope of the information that must be included.

2. In order to ensure meaningful participation of employees and their representatives, ADM systems should be expressly included in the scope of existing collective participation rights.
3. Mandatory constitution of employee representation with collective rights (not the case in Switzerland, for example).
4. Institutionalized cooperation between the employer and the workforce in the form of a commission for occupational health and safety and for participation, made up of equal numbers of members of the employee representatives and the company management. One could also form additional appropriate personnel representations and give them effective participation rights to ensure the participation of employees in relation to ADM systems and data processing.
5. Explicit right of the employee representatives to consult an internal or external expert (as provided for by German law[40]).

II. Continuously enabling employee objections

The opportunities for employees and their representatives to lodge objections regarding ADM systems must be improved. This could be achieved, for example, through the following measures:

1. Clarification of the employee representatives' right of action, i.e. the employee representatives should have the capacity to be a party and to litigate or have partial legal capacity and to conduct collective legal disputes and to submit collective complaints on behalf of groups of employees.

40 §80 para. 2 and 3 *Deutsches Betriebsverfassungsgesetz*.

2. The financing of collective complaints would also have to be regulated.
3. Granting employee representatives access to, or insight into, processed data would help reduce the flood of information at an individual level. Thus, we propose the right of employees and their representatives to access all individual-level data collected, used, processed or created by ADM systems (provided that the data subjects consent), as well as the right to transfer the data in a structured, common and machine-readable format, as known in art. 20 GDPR.
4. Sanctioning a violation of the right of participation through administrative-criminal fines.
5. Protection against dismissal or no acceptance of unfair dismissal if employees refrain from using or participating in the development of ADM systems.
6. Better collective enforcement could be achieved through intervention by labour inspectorates.

III. Structures for oversight and control/enforcement

The suggestions listed here are to be understood as a possible and non-exhaustive sample of options for structures for supervision and control:

1. Mandatory anchoring of corporate due diligence obligations (see V.) regarding the establishment and implementation of risk identification and risk management.
2. Use of impact assessments before and during the development, introduction and use of ADM systems to keep negative consequences as low as possible, with the involvement of employees or their representatives.
3. Regular reporting ("reporting") and thus transparency about identified risks and measures taken to eliminate these identified risks, including impact measurement, and an accountability report on the effects and the well-being of employees.
4. Creation of appropriate control and supervisory bodies.
5. Strengthening the skills and expertise of the National Contact Points for Responsible Business Conduct, which promotes the OECD Guidelines for Responsible Business Conduct.

IV. Solutions empowering social partnerships

Employee participation in ADM systems does not necessarily have to be initiated by the legislature. Before thinking about revision efforts at the legislative level, it is worthwhile to work out solutions within social partnerships. Social partnerships are able to take conscious actions collectively. Due to their proximity to companies and employees, the social partners are particularly predestined to overcome the challenges of ADM systems in the workplace, in a flexible, effective, quick and socially acceptable manner. For decades, many employers and employees have been regulating the working conditions in their company, industry or economic sector on this company-specific or industry-specific basis. The compromises negotiated are tailor-made, pragmatic and, if necessary, consider the individual needs of the contracting parties.[41]

Collective law instruments can therefore be chosen, such as the interaction of social partnerships, the conclusion of works agreements or of collective bargaining agreements. The central element of social partnerships is the collective bargaining agreement, which is the ideal instrument for meeting the need for flexibility. Collective bargaining about the challenging and unclear aspects of ADM systems in the workplace is genuinely within the very nature of labour law. The individual inferiority of the individual employee is compensated for by the collective and its action. Collective bargaining and the conclusion of a collective bargaining agreement allow a relatively low-threshold, democratically legitimated participation in shaping working conditions in the new world of work.[42] Collective bargaining agreements can therefore represent a key to overcoming the challenges of ADM systems by providing an institutional framework with the aim of appropriately balancing the interests affected. However, it seems that this possibility is not often used in practice and is not very well anchored in the consciousness of companies, which is why there is a need to raise awareness on the subject.

41 Isabelle Wildhaber and Raquel Pais, 'Neue Arbeitswelt und Gesamtarbeitsverträge-Plädoyer für einen Rechtsschutz über die Sozialpartnerschaft angesichts der Herausforderungen der neuen Arbeitswelt' in Claudia Seitz, Ralf Michael Straub and Robert Weyeneth (eds), *Rechtsschutz in Theorie und Praxis* (Helbing Lichtenhahn 2022), 542.

42 ibid.

E. Suggestions to address ethical requirements in digital vulnerability of employees

The restoration of human agency requires a space for meaningful ex ante and continuously on-going/ex post representation of employees in the form of grievance mechanisms regarding the implementation and development of ADM systems. To ensure meaningful participation of affected individuals, ADM systems should be explicitly included within the scope of existing information and consultation rights.[43]

I. Key issues to include in an ethical analysis of workplace monitoring

In the following, the ethical analysis focuses on ADM systems in the workplace, building on the findings from the qualitative empirical case studies, which are supplemented by aspects from corresponding expert literature.

1. Deep Insights into privacy and possible monitoring of employee activities

Data-driven technologies now permeate almost every aspect of business life: our qualitative case studies showed that Swiss employees are in daily contact with or controlled by ADM systems.[44] The impact on employees' privacy is also discussed in the literature as one of the most serious ethical problems of datafication in the workplace.[45]

Although the concept of privacy is expressed in different ways in different legal systems, it protects the right to respect for private and family life, home and correspondence (see art. 8 ECHR). Big data analytics in human resource management have a significant impact on the privacy of employees and may lead to abuses/harms.[46] The right to privacy underpins

43 Adams-Prassl and others, 'Regulating algorithmic management: A blueprint'; OHCHR, 'Guiding Principles on Business and Human Rights'; B-Tech, 'Key Characteristics of Business Respect for Human Rights'.

44 Jean-Philippe Deranty and Thomas Corbin, 'Artificial intelligence and work: a critical review of recent research from the social sciences' (2022) AI & SOCIETY 1.

45 Ebert, Wildhaber and Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection'.

46 Alexandra Mateescu and Aiha Nguyen, 'Algorithmic management in the workplace' (2019) 8 Data & Society 1.

and is closely linked to other fundamental rights in the workplace, such as freedom of association and freedom of speech.[47]

Invasions of the right to privacy can be problematic with respect to participation, particularly when the employer is able to obtain insights into communications and potential mobilization activities of employees in the workplace. A free exchange among employees is hardly possible if communication processes or assembly patterns are monitored.

2. Timing of information and consultation

The employer should consult with employees early in the decision-making process, ideally before a decision is made to introduce ADM systems. The earlier discussed UNGPs call for the structural involvement of affected stakeholders as part of human rights due diligence. This can ensure that employees have a meaningful opportunity to participate in the discussion early in the process when important decisions are made and that their views are considered. Experts also suggest the involvement of independent, ethical expert panels.

Thus, data does not tend to be organized by people in discrete and complete ways that are coherent with the understandings that software designers have of computer systems. Data also does not necessarily fit with processes of audit and governance. Moreover, as is well established in critical data studies[48], data is not an entity with objective meanings that can be stolen. Rather it is contingent, in its meanings and in the ways that it is organized.[49]

3. Data competence / data literacy

To enable employee participation, it is essential that employees have an appropriate level of basic knowledge about data processing, analysis and possible bias effects as consequences. Employee data literacy is critical to informed participation in the use of ADM systems. Only when workers can

47 Christoph Grabenwarter, *European Convention on Human Rights: Commentary* (Bloomsbury Publishing 2014), Art. 8 ECHR N 82.

48 Danah Boyd and Kate Crawford, 'Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon' (2012) 15 Information, communication & society 662.

49 Pink, Lanzeni and Horst, 'Data anxieties: Finding trust in everyday digital mess', 12.

understand and interpret the data collected by monitoring tools can they exercise informed voice in participation processes and gain agency over the use and interpretation of their data.[50]

Illustratively, a study[51] demonstrates that human decisions triggered positive emotion as employees connected human decisions with a possibility of social recognition, while algorithmic decisions had a mixed response in the sense that algorithms were seen as helpful but also offering a tracking possibility. So employees perceive digitally permeated decisions differently from human ones. Equally task characteristics differed,*"in particular, perceptions of whether tasks require more "human" or more "mechanical" skills significantly influence how people perceive algorithmic decisions compared to human-made ones. With tasks that mainly involve mechanical skills, participants trusted algorithmic and human decisions equally, found them fair, and felt similar emotion toward them, consistent with our hypotheses. While the degree of perceived trust, fairness, and emotion was the same between algorithmic and human decisions, the reasons behind people's perceptions differed. With human-made decisions, participants attributed fairness and trust to managerial authority; with algorithmic decisions, to reliability and the lack of bias. For the human-made decisions, some participants mentioned the manager's social recognition as a factor that could positively influence workers' emotions. For algorithmic decisions, on the other hand, participants mentioned that algorithms could act as tools to help workers complete their tasks, which could positively influence workers' emotions; or workers might feel negatively about algorithms, if they felt they were being watched and monitored."*[52]

Such studies suggest that it matters greatly for employee perception and for the orgnization's perception of digital vulnerabilities how decision-making and task design is done.

4. Data transparency

Data transparency is an often-discussed factor in enabling employee participation. It is important that employees have access to the data collected

50 Helen Kennedy, Thomas Poell and Jose van Dijck, 'Data and agency' (2015) 2 Big Data & Society 1.

51 Min Kyung Lee, 'Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management' (2018) 5 Big Data & Society 1.

52 ibid, 11.

and in a format that allows them to understand what information is being collected and how it is being used. Companies should ensure that their employees have access to the relevant data and that it is prepared in a format that corresponds to their individual data skills for comprehension. Clear communication of data collection and presentation of how data is handled is a basic requirement so that employees can take part in participation processes. From a technical perspective, it can be complex or impossible to make ADM-supported processes completely transparent, as some technologies are acquired from third-party providers, sometimes from abroad. When using so-called "off-the-shelf" products, the employer does not know exactly which information about employees is measured in which way and what are possible weaknesses of the technology, for example with regard to the measurement quality, because the manufacturer does not provide this information in a completely transparent manner.

5. Clarification about the scope of application of the ADM systems

Since the majority of ADM systems are not developed in-house but are sourced from external providers, this can have an impact not only on data transparency but also on the traceability of decisions. The traceability of decisions must be a core component of an employee participation process.

Clear disclosure of the scope of ADM systems in the workplace is of great importance for employees in order to understand the extent to which they are affected. It is important that employees know in which areas their work is subject to monitoring with the help of ADM systems and what options are available to them to deal with these ADM systems. It is necessary to provide information about which processes, and objection options can be initiated if problems or conflicts arise around the ADM system, both in the introduction process and in daily use.

6. Avoiding «black box systems»

A frequently discussed phenomenon in ADM systems is the genesis of so-called "black box systems".[53] Data-driven ADM systems are being introduced that lack transparency about their decision-making. Employees often must accept extensive data collection about themselves, while the

53 Ifeoma Ajunwa, 'The "black box" at work' (2020) 7 Big Data & Society 1.

details of decision-making are shrouded in secrecy. This can make the employer's ADM-based decisions highly opaque for employees and make it more difficult for them to have a say, as the necessary information base, including consultation, is missing. Employees are thus confronted with a lack of transparency, e.g. regarding discrimination/distorting effects, accountability or explanations about the functioning or even the logic of the "black box" at work.[54] The traceability and fairness of an ADM model can only be achieved through reducing employee vulnerability by ways of technical methods and their communication to employees, so that exchanges about potential for improvement are possible. Here, it is important to rely on collaborative management systems and promote diversity so that different expert opinions make the system more robust and resilient for the benefit of employees, both from a technical, from a labour law and from an ethical perspective.

II. Opportunities at company level to implement due diligence

In general, ethical responsibilities of companies can be derived from the Business and Human Rights Framework, centred around the UNGPs, as described earlier.[55] In addition to the state's duty to protect people from human rights violations by private individuals, the UNGPs postulate a corporate responsibility to respect human rights and to participate in redressing human rights abuses that a company is linked or contributing to. To re-state, the UNGPs have become the de-facto global standard for responsible business conduct and are in line with the OECD MNE Guidelines Enterprises, as briefly sketched prior.

It would be conceivable for the employer to have a duty of care, similarly to the one conceptualized in the UNGPs. This duty of care would include that the employer and the employee representative (or the responsible union) establish a process for exercising human rights due diligence with a focus on the rights of employees at an early stage before the introduction or development of an ADM system. The duty of care would also include regular reporting on the effects on employees based on impact assessments with the involvement of those affected, and an accountability report on

54 Bert Heinrichs, 'Discrimination in the age of artificial intelligence' (2022) AI & society 1.

55 OHCHR, 'Guiding Principles on Business and Human Rights'.

the well-being of employees, as well as measuring the efficiency of the protective measures taken.

The building blocks of the necessary due diligence steps in the context of an ADM system in the workplace are described below and consist of four steps.

1. Identify and assess impacts to assess the nature and extent of human rights

In particular, step 1 of the duty of care is often carried out in the form of a so-called "impact assessments". The impacts of complex ADM systems are often difficult to predict and difficult to manage ex post, so the quality standard must be high, regarding the scope and quality of human rights ex ante and ex post analysis of potential risks of ADM systems as well as regarding the review and implementation of appropriate risk reduction strategies. A thorough internal record of the impacts of ADM systems is important to enable regular impact assessments. This should be done annually or as needed throughout the entire life cycle of a system, and also when additional tools are introduced, in order to avoid negative cumulative effects.

Step 1, derived from the UNGPs for the context of the use of ADMs in the workplace, should include, among others, the following elements:

- Systematic description and assessment of the relevant impacts and risks through reference to qualitative and quantitative information about the use of the ADM systems;
- All "system level" information that is to be made available to employees, and the manner in which it is made available;
- Employers should consult employee representatives and relevant expert groups when identifying the risks and possible protective measures ("stakeholder engagement"). The views of employee representatives and expert knowledge must be taken into account and included. The perspective of those who are potentially severely affected by the impacts should be given appropriate weight. Mandatory collective participation is recommended.[56]

56 Adams-Prassl and others, 'Regulating algorithmic management: A blueprint'.

2. Act to prevent and reduce human rights risks, also through integration into internal functions and processes

The UNGPs were designed to establish a global expectation of responsible business conduct. To this end, the UNGPs require a company to take positive and proactive steps to review, improve and, where appropriate, transform its own business practices and cultures. This also includes the expectation that companies try to encourage employees, business partners and others to act responsibly and with respect for all human rights. When it comes to technology use, this focus on improving new business practices and relationships when dealing with ADM systems in people management is critical.

Step 2 should include, but is not limited to, the following elements[57]:

- Description and assessment of all existing protective measures to mitigate human rights risks in the context of ADM technologies;
- Gap analysis, where existing measures do not cover risks;
- Identification of new measures where gaps have been identified;
- Prioritization of measures according to the "severity of risks".

3. Track the effectiveness of risk reduction measures over time

Companies must assess the effectiveness of their measures to address human rights risks. As a third step in the human rights due diligence process, the UNGPs (UNGP 20) set the following requirement: "In order to verify whether negative impacts on human rights are being addressed, companies should monitor the effectiveness of their response." Follow-up should be based on appropriate qualitative and quantitative indicators and use feedback from both internal and external sources, including affected stakeholders.

For example, a measure could include training by companies for the workforce if ADM systems are used. Targeted training of employees in data analysis and interpretation can help improve their data skills and give them the necessary confidence in dealing with the planned or implemented ADM systems.

57 B-Tech, 'Taking Action to Address Human Rights Risks Related to End-Use'.

Step 3 should include, but is not limited to:

- Impact measurement: Assessment of the effectiveness of new and existing protective measures, including
- Assessment of adequacy: assessment of whether they are appropriate to the impacts and risks;
- Feedback to stakeholders: description of the consultations carried out with employees and their co-workers and disclosure of changes made in response to the views expressed.

4. Appropriate communication of the measures with a view to dealing with human rights impacts

The UNGPs state that companies "should be accountable for the way they manage their human rights impacts" and "be prepared to communicate this externally, particularly when concerns are raised by or on behalf of companies." affected stakeholders" (UNGP 21). The UNGPs state that "communication may take various forms, including face-to-face meetings, online dialogues, consultations with affected stakeholders and formal public reports".

Communication and reporting should focus on the impacts of ADM systems on employees that have been identified. However, communication and reporting must also include transparency about the remedial measures the company has taken to address the impacts and an assessment of the effectiveness of these measures.

Step 4 should include, but is not limited to:

- The impact assessment should generally be communicated publicly, apart from confidential technical and commercial information.
- The impact assessment should be available to employees and their representatives.
- Cooperation with supervisory authorities with appropriate measures to protect confidentiality if irregularities have occurred.

For any disclosure, especially of a public nature, care must be taken to ensure that the information is provided in a suitable manner and format that is easily accessible in order to make it comprehensible.

F. Conclusions

This chapter showed empirical insights about workplace practices around digital technologies and its impact on employees using quantitative and qualitative data about the implementation processes and use of algorithmic management tools in Switzerland. It explored how such practices impact employee perceptions of digital vulnerability. The chapter discussed the key legal foundations on an international level and addressed key ethical aspects and proposed several avenues for solutions.

By showing empirical insights into impacts of current digital workplace monitoring practice on employee vulnerability and proposing matching avenues for solutions, this chapter contributed to exploring how digital vulnerability of employees in digitally permeated workplaces can be reduced. We contextualize the discourse in legal and critical data studies about implications for labour law and ethical challenges.[58]

Further research could explore empirical results from other countries and whether they replicate or differ from the presented data, and to which extent our proposed solutions could help to address the identified digital vulnerabilites of employees.

58 Ajunwa, 'The "black box" at work'; Benedetta Brevini and Frank Pasquale, *Revisiting the Black Box Society by rethinking the political economy of big data* (SAGE Publications Sage UK: London, England 2020); Rogers, 'Workplace Data and Workplace Democracy'; Adams-Prassl and others, 'Regulating algorithmic management: A blueprint'; Ebert, Wildhaber and Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection'; Ajunwa, Crawford and Schultz, 'Limitless worker surveillance'.