Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June: 1–14
© The Author(s) 2021
DOI: 10.1177/20539517211013051
journals.sagepub.com/home/bds
SAGE

Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection

Isabel Ebert[1], **Isabelle Wildhaber**[2] and **Jeremias Adams-Prassl**[3]

Abstract

Data-driven technologies have come to pervade almost every aspect of business life, extending to employee monitoring and algorithmic management. How can employee privacy be protected in the age of datafication? This article surveys the potential and shortcomings of a number of legal and technical solutions to show the advantages of human rights-based approaches in addressing corporate responsibility to respect privacy and strengthen human agency. Based on this notion, we develop a process-oriented model of Privacy Due Diligence to complement existing frameworks for safeguarding employee privacy in an era of Big Data surveillance.

Keywords

Employees, workplace, surveillance, privacy, data

Introduction

Data-driven technologies are increasingly gathering and processing data across the full spectrum of contemporary society and human activity. This datafication touches on most areas of life (Cukier and Mayer-Schoenberger, 2013; Neff and Nafus, 2016). It is not surprising, then, that Human Resource Management has similarly begun to embrace datafication for its core processes. Companies are increasingly attracted by the promise offered by data analytics to monitor the behaviour and performance of their employees in the workplace, sometimes even extending to non-job-related behaviour. 'People Analytics' vow to take human resource management practices to a new level. Often, there is also an underlying belief that technology might make people management decisions more objective, efficient and less prone to serving individuals' preferences (Finlay, 2014). As a result, the monitoring of employees on a minute-by-minute basis increasingly affects employees across a range of industries (Ajunwa, 2020; Ball, 2010; Mateescu and Nguyen, 2019; Prassl, 2018).

The object of monitoring/surveillance also extends across employment grades and pay levels, from call centre workers to senior managers, and increasingly affects 'thinking work' (Phan et al., 2017). For instance, banks in the City of London rely on surveillance technology to see whether employees are present or not (Morris et al., 2017). Some companies even use more physically invasive methods of surveillance, such as microchip implants that connect employees to the company network (Astor, 2017).

The global spread of COVID-19 in the spring of 2020 has dramatically accelerated the use of workplace analytics, for at least two reasons: first, because many of the technologies involved in datafying the workplace are now being deployed and/or repurposed for public health protection, such as monitoring workers' social distancing in factories and warehouses (Vincent, 2020). Second, the dramatic growth of home working has significantly increased demand for software solutions that offer remote surveillance and management possibilities, taking the datafication of work right into individual homes (Collins, 2020; Frantziou, 2020).

---

[1] Institute for Business Ethics, University of St. Gallen, St. Gallen, Switzerland
[2] Institute for Work and Employment Research, University of St. Gallen, St. Gallen, Switzerland
[3] Faculty of Law, University of Oxford, Oxford, UK

Corresponding author:
Isabel Ebert, Institute for Business Ethics, University of St. Gallen, Girtannerstrasse 8, St. Gallen 9010, Switzerland.
Email: isabel.ebert@unisg.ch

These dynamics raise major ethical questions, including notably the broader shift from human to algorithmic decision-making (Mittelstadt et al., 2016). In addition to these ethical challenges, companies face significant legal risks, as they struggle to map and mitigate the legal implications new technologies used for workplace monitoring might have on their employment relationships (Ajunwa et al., 2016). Yet, at the same time, workplace monitoring is becoming the new normal (Kellogg et al., 2020). Emerging scholarship has demonstrated that workers are increasingly confronted with a 'black box' at work, lacking transparency, accountability, or explanation about monitoring practices (Ajunwa, 2020; Pasquale, 2015). A major concern emerging from the current literature centres on the protection of privacy (Bhave et al., 2019) and related questions surrounding accountability structures, transparency about information sharing, and potential discrimination (Ajunwa et al., 2016; Boyd and Crawford, 2012).

Whilst expressed in a number of distinct ways across different jurisdictions, the concept of privacy ultimately protects the right to respect for private life, family life, home and correspondence (for an influential illustration, see European Convention on Human Rights, Art. 8). Big Data analytics in human resource management heavily impact employee privacy and can lead to privacy breaches, infringements and violations (Mateescu and Nguyen, 2019). The right to privacy underpins, and is closely connected to, other fundamental rights at work and beyond, such as freedom of association and speech (Grabenwarter, 2014). To respond to this multi-layered challenge of managing employee privacy at the workplace, we suggest solutions might be found in both legal and ethical scholarship to address transnational challenges for the 'data citizen' (Guild, 2019). A multi-disciplinary and global approach is needed to address privacy protection in a world where workplace monitoring is quickly becoming the new normal (Kellogg et al., 2020).

The privacy implications of this significant increase in the uptake of workplace monitoring technologies, as well as its managerial and legal implications, have so far been relatively underexplored in a solution-oriented analysis which looks beyond a particular regulatory regime or jurisdiction (Collins, 2020; Frantziou, 2020). In this article, we address this gap by conducting a critical inquiry into privacy issues in workplace monitoring, as well as exploring why a human rights-based due diligence approach is suitable to protect employee privacy. This approach serves as a complementary, holistic framework to existing legal and technical approaches, including data protection and Privacy by Design (PbD). We propose a Privacy Due Diligence approach that allows companies to develop a systematic mechanism to handle privacy issues in the workplace as an on-going practice, tailored to individual business models and workplace settings. The proposed Privacy Due Diligence model goes beyond a purely legal or technological solution: our model offers a dynamic managerial process to address privacy issues at the data-driven workplace as they arise, and empowers workers' data autonomy. By taking a multi-disciplinary stance anchored in strong stakeholder engagement mechanisms, our model furthermore ensures that the perspectives and needs of all affected groups are included in dialogue at the managerial level.

To this end, we argue that a set of mechanisms from the 'Business & Human Rights' (B&HR) literature can address corporate responsibility to respect privacy at the workplace (Ruggie, 2007, 2013; Wettstein, 2015, 2016). Human rights due diligence is widely discussed in the B&HR scholarship and offers a rightsholder-centric approach for corporate management (Ebert et al., 2020; OHCHR B-Tech, 2021). A B&HR perspective is enhanced by ethical demands in addition to legal compliance. Its benefit lies in multi-disciplinary, process-oriented managerial tools and implementation strategies based on clearly defined human rights norms, namely the UN Guiding Principles on Business & Human Rights (UNGPs; United Nations Human Rights Council, 2011). Rather than offering static solutions, such as design options, one-off risk assessments, or *ex post facto litigation* once rights violations have occurred, the Privacy Due Diligence approach is conceptualized as an on-going, systematic process that corresponds to the fast pace of technological progress. Policy makers increasingly refer to the UNGPs for governing technology as a normative consensus on the corporate responsibility to respect human rights (Council of Europe 2020).

Our discussion is structured as follows. A first section provides illustrations of workplace surveillance and algorithmic management techniques, highlighting employee privacy issues along the data life cycle, from collection to erasure. We then survey existing frameworks for employee protection, from legal to design-based approaches, highlighting their strengths and identifying a number of weaknesses. It is on the basis of that discussion that we then turn to the B&HR approach as a way of providing a structured process to map risks, identify privacy gaps and anchor privacy due diligence in corporate practice.

Employee privacy issues along the life cycle of data

Algorithmic management has come to augment, or even replace, the full gambit of traditional employer functions (Trade Union Congress, 2018): whilst hiring is perhaps the most visible use of algorithmic management to date, the use of Big Data HR extends to scoring workers' productivity (Heaven, 2020), tracking day-to-day work behaviour and even terminating employment relationships by firing workers with low 'rates' as determined algorithmically (Steele, 2020). Whilst present space limitations prohibit a detailed descriptive account of these technologies (Neff et al., 2020), suffice is to say that the rapid growth and expansion of algorithmic surveillance and management at work is bringing about a significant shift in work organization.

It is not difficult to imagine the ensuing risks of privacy infringement. A large range of industries aim to monitor and, to a certain extent, predict individual future behaviour using data analytics, e.g., to determine the employees' mood and willingness to exert a task (Eubanks, 2018; Waddell, 2016). Some companies, for example, use neural networks to connect and analyse large data sets (Cheekoty, 2019). These techniques can convey profound insights about individual preferences and behaviour, but are often criticized as not being fully retraceable (Monahan, 2016; Pasquale, 2015). Employee privacy is at stake throughout the entire life cycle of data (European Parliament Position, 2014: Recitals 71a, 71b, Art. 23 para. 1, Art. 33 para. 3), which can be broken up in four phases with regard to privacy concerns resulting from data processing (Tamò-Larrieux, 2018):

1. During *data collection*, employees might experience surveillance, a lack of transparency and awareness about data collection taking place, potentially being the object of significant power imbalances (Felzmann et al., 2019). Employees' freedom and autonomy to exercise adequate control over their privacy with respect to data collection might be limited or lacking.
2. Employees might not be informed about *data analysis* due to knowledge asymmetry. An analysis might contain errors, result in misrepresentation/bias of individual employees or groups of employees (Hong, 2016) and dehumanize human interaction.
3. *Data use* as the basis of decision-making may lead to discrimination of a group of employees or individual employees or a lack of autonomy about the implementation or use of data.
4. During *data erasure*, a company might disregard the importance of 'forgetting' employee data and might lack autonomy, transparency and accountability when dealing with the erasure of employee data.

Misconduct with regard to the use of data can result in a so-called 'function creep', meaning that the data collected is used for other purposes than previously communicated (Christl, 2017). Furthermore, data information might be an issue, as often employees find themselves in a weak position to demand transparency or insight into certain analytics practices that use their personal data.

The inherent conflict between datafication and privacy

The more data is collected about individual employees, the more valuable it gets for predictions based on these techniques. Whilst datafication technologies, such as AI, build on large amounts of data for increased accuracy of results, many privacy provisions would call for alignment with the data minimization principle (e.g. taken up in GDPR Art. 5) that stands fundamentally at odds with Big Data techniques. This is a tightrope walk for any organization: Whereas compliance or corporate governance departments might call for privacy as a high priority, business intelligence and HR management might be highly interested in collecting and processing as much data as possible (Koops and Leenes, 2014).

Existing frameworks for the protection of employee privacy at the workplace

In the following, we explore selected current frameworks for the protection of employee privacy in the workplace, highlighting the potential of both legal and technological solutions in resolving the inherent conflict of interest between Datafication and Privacy. We also identify a number of potential shortcomings in both legal and technical solutions, as set against the background of broader socio-technical notions of privacy and workplace monitoring.

Legal protection of employee privacy at the workplace

The applicable law to an employment contract and to an individual employee always relates to a specific jurisdiction. Whilst companies may be held accountable for privacy infringements in the workplace based on national labour or data protection laws, records of personal data seem to float freely across jurisdictions. Companies perceive increased pressure to deal with privacy issues at the international level, partly due to new legislation in Europe, the US (California Consumer Privacy Act (CCPA), 2018) or also Brazil (CCPA, 2018; Singer, 2019; Thomas, 2019). Therefore, data-driven workplace monitoring is a phenomenon affecting data sharing practices beyond a nation's border. Multinational companies operating in several jurisdictions with multiple privacy standards will strive to find a solution that protects privacy across geographies (Bhave et al., 2019; Guild, 2019).

A growing body of scholarship is exploring the role of privacy and data protection in the context of work, with a particular emphasis on European regulatory regimes (Brassart Olsen, 2020; Otto, 2019; Simitis, 1999). Given the EU's early regulatory invention, there is clear potential that the so-called 'Brussels Effect' (Bradford, 2020) will lead to spill-overs of similar legislation in jurisdictions beyond European borders. A number of distinct yet overlapping and closely intertwined legal regimes in Europe aim to protect aspects of employee privacy, including the European Convention on Human Rights (1953), the European Union Data Protection Regulation (GDPR, 2016), the EU Charter of Fundamental Rights (2012) and national employment law regimes. One aspect of privacy, the respect for private life is required by the European Convention on Human Rights of the Council of Europe (1953) as well as national legislation: The respect for private life also extends to privacy in the workplace, as recognized by the European Court of Human Rights in Niemitz v. Germany (1992; Grabenwarter, 2014). Moreover, data protection law in the form of the GDPR addresses privacy issues resulting from datafication in the workplace (see also EU Directive (EU) 2019/1152; see further Otto, 2019). The GDPR is directly applicable to private actors within the EU member states and even has some extraterritorial effects (GDPR). Information about the workforce can only be 'collected for specified, explicit and legitimate purposes' (GDPR, Art. 5(1)(b)); there are further safeguards in place for sensitive data, including 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership' (GDPR, Art. 9(1)).

Perhaps the strongest safeguard can be found in GDPR Article 22(1), which grants workers the 'right not to be subject to a decision based solely on automated processing ... which produces legal effects concerning [them] or similarly significantly affects [them].' As the WP29 Guidelines EU General Data Protection Regulation (GDPR) Regulation (EU) (2016) make clear, this provision is to be interpreted widely: it will not be sufficient, for example, merely to 'fabricat[e] human involvement'. In an employment context, it would appear that the deployment of automated scheduling software and other management tools falls within the Article 22 prohibition, as they will frequently involve 'decisions that deny someone an employment opportunity or put them at a serious disadvantage' (WP29, WP 251rev.01: 22). That said, Article 22 also provides for a number of exceptions.

Other scholars have also elucidated a 'Strasbourg Effect' similar to the 'Brussels Effect' by the GDPR (Bygrave, 2020), tending from the regional level (Council of Europe Recommendation No. R (89) 2 and Rec (2015)5; WP29, 2001, 2002, 2017) to the international level. The right to privacy in the workplace has also been recognized in concrete terms at a universal level (International Labour Organization, 1997) efforts to extend the responsibility for respecting human rights by obliging private companies to ensure compliance with international human rights norms are increasingly becoming visible at the international level (Kälin and Künzli, 2019). One reason for this is that private companies, including tech industry companies, have gained powerful agenda-setting power ever more resembling a state actor: private companies using datafication at the workplace have a strong stake in determining the ways in which an individual's life is transposed into quantifiable data (Keats et al., 2014) – and they need to do so responsibly to not violate employees' human rights in the workplace context. Overall, however, no legal regime to date has laid down comprehensive protective standards internationally.

The promises and pitfalls of design-based approaches to uphold privacy at the workplace

A number of solutions based on tech-design have also been proposed to complement existing legal frameworks for the deployment of people analytics software – though they are not necessarily able to provide a complete solution to the concerns we have identified. One such tech-based approach to provide better privacy protection across borders by embedding design specifications of information technologies, accountable business practices and networked infrastructures is PbD (Cavoukian, 2012; Koops and Leenes, 2014; Rubinstein, 2012). PbD has the potential to protect personal data and prevent legal proceedings. It departs from a decentralized set-up of safeguards against privacy issues, potentially suitable for privacy protection of transnational people management practices (Koops and Leenes, 2014).

The expectations for PbD from scholars from different continents and disciplines are high: PbD is described as a pragmatic compliance enabler to guarantee important elements of procedural regularity (Kroll et al., 2017; McQuay and Cavoukian, 2010). Some scholars claim that it will be difficult if not impossible to achieve meaningful privacy protection in the 21st century without PbD (Dix, 2010). Indeed, design-based approaches are popular even beyond the tech industry and have increasingly found their way into legal frameworks. According to the GDPR, data protection by design is an 'appropriate measure' to comply with data protection law (GDPR, Art. 25 para. 1). The European Court of Human Rights (ECHR) has been relatively early in embracing ideas similar to those of PbD, such as in I v. Finland (2008).

Yet, the claim that design-based solutions within the current legal structures alone can provide sufficient privacy protection has been contested in the light of ongoing technological progress (Koops and Leenes, 2014; Rubinstein and Good, 2013; Spiekermann, 2012). There are three overarching reasons why existing legal frameworks and/or tech-design approaches can offer only limited protection to prevent an infringement of privacy in the context of workplace monitoring.

Missing contextuality for proportionality & consent. At present, it is not conceivable that a specific design can respond to legal situations where *all circumstances or the context,* respectively, need to be taken into account. Such context is important where the proportionality of a privacy-intrusive measure or the voluntariness of consent is at stake.

The principle of *proportionality* is well established in the jurisprudence of the ECHR, in national and European Union law. The fair balance test between the interests of the employer and the employee with the consideration of all circumstances has been a central element in three key cases regarding privacy at the workplace at the ECHR: Köpke vs. Germany (2010) focussed on video surveillance of a supermarket cashier suspected of theft. The ECHR found there was nothing to indicate domestic authorities had failed to strike a fair balance between the applicant's right to respect for her private life and both her employer's interest in the protection of its property rights. In *Bărbulescu vs. Romania* (2017), the Grand Chamber of the ECHR found that the monitoring of an employee's email account resulted in the violation of his right to respect for private life and correspondence. In López Ribalda and others vs. Spain 1874/13 and 8567/13 (2018) discussed covert video surveillance of supermarket cashiers and sales assistants by employers. Reviewing earlier events during the employment relationship, the employment courts decided the interference with the applicants' privacy as proportionate. Over time, a different weight may be given to the competing interests concerned, having regard to the extent to which intrusions into private life of workers are made possible by new, more sophisticated technologies (see Köpke vs. Germany, 2010). However, a design-based approach tries to tackle data protection problems ex ante. Algorithms do not work with all circumstances that would have to be taken into account in order to judge the legality of a measure. As limited computational programmes which are restricted to perceive and process predetermined data, algorithms cannot perceive the environment the way humans can – no matter how sophisticated the tech-design. For these reasons, design-based approach cannot adequately incorporate the principle of proportionality and cannot ex ante balance the interests for the moment in time of decision-making (Keats Citron and Pasquale, 2014).

In addition to proportionality, consent is a factor of major concern in the workplace setting. *Consent* should be prior, informed and free and hence requires very specific information about the context of the collection and use of data. Free consent can be in doubt, and thus, invalid, in situations of subordination, where there is a significant economic or other imbalance between the controller securing consent and the data subject providing consent (European Union Agency for Fundamental Rights, 2018: 397). As the recitals to the GDPR make clear, consent should not provide a valid legal ground for the processing of personal data in situations of imbalance between the data subject and the controller (GDPR, Recital 43), e.g., between the employer and her employees, consent does not justify the processing of personal data, unless in exceptional situations (WP29 Opinion, 4). The circumstances under which consent is given should therefore be carefully considered when assessing the validity of consent in the employment context (European Union Agency for Fundamental Rights, 2018: 332). Therefore, employees need to have a real choice between giving consent or not. A PbD approach will likely not be able to integrate all factual details and circumstances relevant to judge the legality of a given consent. With regard to the scope of monitoring practices, it is important to ensure that workplace monitoring needs to be limited to its 'appropriate context – actual workplaces and actual work tasks' empowered by a boundary that could not be breached through 'notice-and-consent mechanisms', as Ajunwa et al. (2017: 774f) have argued.

Blurry legal terminology translated in code. A second obstacle for design-based approaches is the lack of consensus about the meaning of legal terms. It is difficult for a computer programmer to translate legal concepts into code if the respective legal rule builds on vague legal terms. The concept of PbD consists of not one, but two unclear terms: *privacy* and *design*. Some legal scholars, for example, now try to define privacy in a way that is more susceptible for computer scientists: one proposal includes a design strategy which defines the conceptualization of privacy to a narrower, more accurate and attainable concept of obscurity (Hartzog and Stutzman, 2013). Along with this, for example, there is no widely accepted definition of privacy-enhancing technologies (Kroener and Wright, 2014). Also, the notion of PbD is criticized as vague, amorphous and recursive (Bygrave, 2017; Rubinstein, 2011). Norms that are too abstract will not be effective (Martini, 2018). The blurred terms make it difficult to analyse the precise effects of PbD and which law might be applicable.

Technological progress outpacing design-based privacy protection measures. The current state of technological development can overhaul the possibilities of PbD over time. On the one hand, the technology meant to protect privacy today is developing more slowly than newly invented privacy-invading technology (Montjoye et al., 2013). As a result, gaps in protection are omnipresent. However, the lack of technological advancement might only be a temporary problem. On the other hand, the technology of today might not protect against privacy issues caused by the technology of tomorrow, such as the risk of anonymization not being effective due to potential re-identification in Big Data environments (Rocher et al., 2019): So, there is a leapfrog gap between privacy-invading technologies and privacy-protecting technologies.

In sum, just as we saw the promises of particular legal solutions, PbD is an appealing and widely accepted strategy of the digital age to protect employee data. However, we have identified why PbD offers only limited privacy protection at the workplace. We must therefore search for an additional protective approach which will be complementary to, rather than exclusive of, existing approaches.

A broader privacy approach is necessary. We have shown that PbD with its tech-based solutions is *no panacea* because there is no simple fix for complex privacy challenges (Dix, 2010; Hartzog, 2018). Whilst companies have an interest in ensuring the employee productivity and preventing misconduct in the workplace, the measures to uphold that interest do not justify extensively invasive practices for quantifying the social modes of interaction and connected performance goals (Ajunwa et al., 2017). Also, data-driven models that quantify human behaviour are not immune to errors or false conclusions about human interaction (Nagy and Neff, 2016) and are often embedding developers' social assumptions and underlying societal beliefs (Ustek-Spilda et al., 2019). That is why potential cumulative risks through 'toxic combinations' for privacy stemming from different business purposes need to be detected and mitigated with an actual human assessment. For example, data for health prevention (i.e. Covid-19) might be combined with data for performance monitoring, and create profound insights into an employee's private life.

An organization has to consider the socio-technical notion of datafication to grasp how and when employees are subject to monitoring technology and how they react to this (Neff et al., 2020).

Organizational measures need to be systemically integrated and follow an on-going, consistent evaluation of potential privacy risks for the entire data life cycle. The key drivers behind the concept of PbD include 'accompanying' organizational measures for accountable business practices but only to a bare minimum. Faced with the scale and intrusive nature of Big Data techniques, these accompanying measures appear insufficient. Privacy-related decision-making cannot happen in an executive management or legal compliance silo. A broader privacy approach is necessary that can also encompass ethical expectations towards the fair treatment of employees by the management deciding about workplace monitoring measures. Representatives from all affected stakeholder groups need to be strategically involved.

The holistic model to uphold privacy at the workplace offered by business & human rights

Understanding how an organization can deploy technology without violating privacy demands knowing how organizational stakeholders make sense of the technology in use and how much agency they have (Nagy and Neff, 2015; Wagner, 2019). A major asset of a human rights-based approach is that the rightsholder serves as the focal point of attention and is not neglected in a 'passive' role as data subject. At the same time, however, it is important to recognize the potential pitfalls of a fundamental rights approach to workplace protection – including in particular the charge of its atomistic nature, reducing worker solidarity, and thus potentially exacerbating the very inequality of bargaining power which triggers the need for protection in the first place (Youngdahl, 2009). One way of addressing that challenge is to ensure that collective as well as individual employee voices are brought back into the conversation through on-going stakeholder engagement, which can include trade unions, works councils, or other worker representation bodies.

The rights-based approach of B&HR calls for the prevention, mitigation and remediation of negative impacts on human rights through all business operations and is applicable to the workplace and towards companies' own employees. It has the following three overarching benefits to protect privacy at the workplace (Alston, 2005; Ruggie, 2007, 2013; Wettstein, 2015, 2016): Firstly, it refers to a universally defined frame of reference with the Universal Declaration of Human Rights and the UNGPs (2011). Secondly, it proposes concrete managerial proposals and processes through human rights due diligence that can connect to existing risk assessment processes within the business to achieve human rights respecting business conduct. Thirdly, the notion of B&HR restates the state duty to protect human rights, also in technology (OHCHR B-Tech, 2021), whilst perceiving the state in a non-static manner, and emphasizing the responsibility of business to respect human rights, such as privacy at the workplace and provide 'human agency' to all affected stakeholder groups by stakeholder engagement (Wagner, 2019).

In the line with UNGPs, all businesses have the corporate responsibility to respect human rights across their business activities. This notion of corporate responsibility under B&HR is distinct from the conceptualization of corporate responsibility in the academic discourse on 'Corporate Social Responsibility' (CSR) or 'AI Ethics': CSR and AI Ethics have no common reference framework and definitions vary from company to company, ranging from voluntary efforts to industry self-regulation (Smuha, 2020). The consequence is that both CSR and AI Ethics have been critiqued as volatile for hiding unpleasant facts ('whitewashing'), rather than addressing root causes or mitigating actual risks (Wagner, 2018). At the same time, the B&HR approach does not neglect ethical considerations but rather ties them to the UNGPs as the baseline to depart from: During the process of due diligence, considerations from the various approaches within the AI Ethics discourse can be integrated (Smuha, 2020).

Due diligence in line with B&HR is not solely a legal or technical process but also a multi-disciplinary managerial stance to uphold ethical values by respecting human rights across company operations and integrating rightsholders' voices (McCorquodale et al., 2017; OHCHR B-Tech, 2021). It can give back agency to humans rather than making them a 'basic rubber-stamping mechanism in an otherwise completely automated decision-making system' (Wagner, 2019). Following the B&HR rationale, companies should carry out due diligence regarding the impact of their business on human rights, including the privacy of employees. Private employers should therefore respect the privacy, along with connected human rights, of their employees. The right to privacy remains closely inter-connected with other fundamental rights and cannot be discussed in isolation from other human rights at the workplace. The protection of personal data is a specific aspect of the right to respect for private life (Grabenwarter, 2014). The essential aim of the Privacy Due Diligence process is, in line with arguments made by Ajunwa et al. (2017: 775), to emphasize the right to privacy of the employee in the light of the employer and allow for employee autonomy over their data and provide for greater data autonomy. Additionally, a solid understanding of the technological state-of-the-art and its analytical capacity is necessary to grasp the dangers of workplace monitoring (Ball, 2010). Based on the requirements of the UNGPs, companies need to formulate policies on privacy at the workplace and implement them using a due diligence process (UNGPs, 2011: Number 15). Human rights due diligence is to be integrated as an on-going process, aiming at on continuous improvement. The focus lies on the rightsholder(s) and is naturally context-dependent, given the space it creates for stakeholder engagement and representation of voices from most impacted. This means that every business has the responsibility to protect its employees from privacy infringements across its operations.

The devil is in the detail. There is no 'one size fits all' for human rights due diligence. This means that a due diligence model focussing on privacy needs to be implemented as part of a wider conceptual human rights understanding at the company level. For the context of workplace monitoring, it is important to emphasize that an intrusion into the private sphere of an individual lays bare the very data that people analytics might use, in particular in data-driven organizations. Hence, upholding privacy can be seen as one of the gateways for human rights protection in the data economy. A violation of privacy can impact other human rights. For instance, workers can be prevented from carrying out a strike or other form of collective form of resistance (right to freedom of association) as they were monitored even whilst still mobilizing for a certain political-social cause (Peterson, 2020). Hence, upholding privacy can be crucial to protect against cascading infringements of inter-connected human rights. For instance, companies need to be aware of their responsibility to protect employees from risks of negative repercussions of privacy invasions on their mental health (Hillmann, 2015).

Introducing privacy due diligence

In the following, we describe how a company can enact privacy protection at the workplace, following a due diligence approach. Our *Privacy Due Diligence concept* is based on the requirements for human rights due diligence in the UNGPs and combines insights from literature regarding privacy and analytics of human behaviour (Ajunwa et al., 2017; Boyd and Crawford, 2012; Keats Citron and Pasquale, 2014; Prassl 2019). We adapt the concept of human rights due diligence and specify the necessary requirements to uphold the protection of privacy at the workplace. This approach goes beyond a design-based approach and pays reference to core principles of data protection law and employment law. In order to achieve this, it is important to note that there is a need to tailor a company's Privacy Due Diligence process to its individual business model. The UNGPs do not offer a template for human rights due diligence as such, and the concept has been operationalized in different ways. Throughout all due diligence steps, the focus rests on the rightsholder and risks of infringing its rights, and to mitigate and remediate potential harms (OHCHR B-Tech, 2021).

The Privacy Due Diligence model we suggest follows a *four-step logic*: (1) Mapping the 'privacy footprint', (2) Privacy gap analysis, (3) Prioritizing measures, impact mitigation and management and (4) anchoring of privacy protection at the workplace. This model incorporates key elements of the GDPR, yet at the same time proposes a dynamic way for management to deal with privacy issues at the workplace in an on-going manner and with strengthened engagement of external stakeholders. This dynamic character is essential to respond to the fast speed of technological progress: 'no one can predict with certainty all of the ubiquitous-computing innovations that the coming years will bring and realizing their full potential will not be easy' (Cascio and Montealegre, 2016: 354).

Mapping the 'privacy footprint'. The first step is to map the scope of privacy concerns. A solid understanding of the technological state-of-the-art and its potential from a technical side is necessary to grasp the privacy footprint. To analyse adverse impacts, it is important to engage with a wide variety of different audiences to understand all privacy implications of a company's workforce monitoring practices. Before processing data in the workplace context, it is vital to ask what the purpose is (purpose specification) and consider data minimization practices. Asking the purpose question should tease out a lot of privacy concerns from the outset (cf. also considerations in step 3).

It is questionable whether an employer should collect vast amounts of data in the first place. Yet, if an employer decides to do so, due diligence should focus not only on data minimization, but also on data quality. To this end, we can apply the *Life Cycle of Data* framework, as previously discussed, to employee privacy at the workplace (European Parliament, 2014: Recitals 71a and 71b, Art. 23 para, 1, Art. 33 para. 3). Affected stakeholders – all stakeholders impacted in their privacy by workplace monitoring technology – might not be just a company's own employees, but also rightsholders negatively influenced through privacy infringements of employees, such as their partners or children. Further, the role of volunteers or agency-workers needs to be taken into account. Where can contract-workers seek remedy or voice concerns? Privacy at the workplace needs to take core principles of data protection law into account, such as: purpose, specification and limitation; prior informed consent; data minimization; and use limitation.

Yet the model of Privacy Due Diligence goes beyond a solid interpretation and application of data protection law: Its checks and balances are oriented towards ensuring the requirements of the UNGPs *beyond compliance and as an on-going process*. Even if an action would, strictly legally speaking, still be tolerable under national law or international standards, stakeholder engagement might suggest a different result. If, for example, the workforce opposes a particular workplace analytics measure very strongly, a company should strive for a reversal or compromise solution instead of pushing through against the will of its staff. Strategic stakeholder engagement forms the basis of B&HR due diligence and differs from mere consultative approaches as it builds onto a rightsholder perspective. In light of technological advancement, certain affected stakeholder groups might not be able to grasp and foresee scathing privacy infringing impacts. Stakeholders might lack the insight or information about technological analytical capabilities on what is being measured and which conclusion could be drawn (function creep). Privacy Due Diligence responds to the bargaining power imbalance problem between the employee and employer as it potentially goes beyond the employment contract terms that parties consented to. The goal of the mapping is to foster the privacy-guided mindset of those responsible for developing and running data processing systems rather than demand compliance by techno-regulation (Koops and Leenes, 2014).

Companies need to grasp where their operations affect employees' privacy most. Key questions include: Which groups are affected by privacy issues and in what ways? Who might be particularly vulnerable? The privacy impact assessment as part of the Privacy Due Diligence should include a hybrid model that consists of both the engagement with internal stakeholders, as well as the strategic involvement of additional external stakeholders.

Whilst, for example, the GDPR proposes a data protection impact assessment (DPIA) to assess how personally identifiable information is collected, used, shared and maintained within an organization (Hartzog, 2018), it neither expressly stipulates an obligation to take the expressed opinions into account, nor includes potentially affected stakeholders, besides data protection officers, the employees and the supervisory authority (GDPR, Art. 35 para. 2, GDPR, Art. 35 para. 9). GDPR DPIAs can be integrated into

Privacy Due Diligence if amended by strategic engagement with potentially affected stakeholders. A solely internal process is at risk of being biased to the companies' interests, whereas a process purely targeted as a reporting exercise to a supervisory authority misses the point of the on-going character of due diligence. Hence, the Privacy Due Diligence approach builds on both external and internal stakeholder involvement.

2. Privacy gap analysis: Identifying existing processes and potential disparities. In this second step, the business sets up an inventory of privacy-protective measures in place in the company to determine where gaps exist with regard to privacy protection at the workplace in data-based management processes. As stressed previously, workplace monitoring needs to be limited to its appropriate context, the actual workplace and the actual work tasks and this prerequisite should not be able to be waived away with notice-and-consent mechanisms (Ajunwa et al., 2017:774f). In this step, some companies might discover design-based solutions to address emerging privacy issues. Yet, as sketched above, tech-solutions only protect against privacy infringements to a certain extent. From a B&HR perspective, a company enters a *grey area of responsibility*. Again here, the engagement with rightsholders is key, requiring proactive, strategic human interaction rather than solely tech-based analysis of a situation (see step 1). The protection of data and privacy is thus not limited to ensuring legal standards, but must also *address ethical issues*. A gap analysis therefore consists of at least two steps:

a. Are all necessary legal requirements met? This includes taking into account the context, proportionality, consent plus establishing clarity of the meaning of legal terms and the technological state of the art of protective measures.
b. Are those ethical challenges with regard to privacy also addressed (legal grey areas) which might lead managers or employees into a socio-technical dilemma?

This gap analysis goes beyond the legal framework and addresses issues arising from regulatory gaps or different legal notions across jurisdictions for a sound company policy on privacy across jurisdictions. There are well-established gap analyses that focus exclusively on the legal dimension and deal with elementary issues such as lawful basis and transparency, or data security. Such gap analyses can easily be integrated into a Privacy Due Diligence approach. However, the systematic handling of such regulatory gaps is more challenging. The gaps identified are highly dependent on the respective business activity, sector, or employee groups.

Providing transparency about analytics models needs to take the technological capacity into account (descriptive, predictive or prescriptive analytics). Further, the privacy gap analysis needs to consider the model's business purpose: For instance, which sample of input data and classification results are selected? Are there exogenous variables that could produce bias when calculating probabilities? Could this result in harm, for instance, for people of colour that will not receive a promotion or might be dismissed due to systemic bias in the data model (Buolamwini and Gebru, 2018)? A managerial decision needs to be taken regarding how to establish transparency and avoid privacy intrusions that can, among other issues, lead to discrimination and adversely impact other human rights. Stakeholder engagement from a due diligence perspective would require that employees are informed about data analytics in a reasonable and proportionate manner to the extent of the analytics measures and have a say about how such systems are implemented (Wagner, 2019).

Privacy Due Diligence can identify and address arising privacy gaps better than a purely legal or technical assessment. For example, 'Hubstaff' offers software recording employees' keyboard strokes, mouse movements and visited websites or 'Time Doctor' takes videos of employees' screens and/pictures through a webcam each 10 minutes to check that employees are at their computer (Heaven, 2020). Many decisions here remain subject to the decision-making inside companies, but should be subject to wider stakeholder engagement practices. Such decisions need to be made in line with human rights requirements, e.g., it is hardly justifiable inferring political opinions, sexual orientation or information about an individual's health by analysing clicking and browsing patterns at the workplace.

Often, rightsholders might not be fully able to anticipate future privacy risks: Particularly in dealing with novel technology, the potential consequences cannot be fully estimated today. It is important to ensure ethical acceptability by considering normative issues emerging from the use of workplace analytics. A legally and ethically demanding gap analysis therefore cannot process an existing catalogue of standardized, formulated items, but requires a deeper reflection based on ethical key questions around the interpretation of what constitutes the right to privacy.

Prioritizing measures, impact mitigation and management. Privacy dilemmas result from a complex interplay of interests and hence do require human judgement and weighing of interests. This allows for coping with situations where design-based approaches fail to deliver proper privacy protection. Room for human judgment is required where the proportionality of an employment relationship needs to be assessed.

The most severe impacts from a rightsholder perspective (salient privacy issues) need to be addressed and acted upon first. Companies need to identify what next steps to take in order to mitigate risks ranked by salience of the privacy risks. For impact mitigation and management, a company needs to outline how the gaps identified in step 2 can be closed for salient privacy issues. For example, Deloitte and Bank of America workers allegedly had to wear badges that recorded everything the workers saw and heard, by analysing the speech of the person wearing the device, its volume and pitch, length of time span spent in a place, and mapping the daily paths enabled by beacons through the office space (Steele, 2020). Whilst all this might sound promising for delivering insights to the people management department, such invasive methods are often barely justified and might not be connected to the actual output that they are supposed to measure (purpose limitation). Asking the purpose question 'I would like to analyse my employees' productivity, so I need this data' should prompt the answer 'Why? On what basis? Why do you need to know about this, isn't that a breach of their privacy?'. For some technologies, the purpose seems clear at first sight but with a closer look embodies salient privacy gaps: For example, smart jackets for first responders can be equipped with modules that monitor the heart rate, temperature, motion and geo location (Steele, 2020). Some modules, such as body cams are active beyond the emergency moment and allow to track the completion of tasks and monitor workflow. Due Diligence might show that this is not an appropriate use of data-driven monitoring when balancing the necessity for monitoring work performance when juxtaposed with the privacy intrusion.

In contrast, a geolocation tracking system that tracks a van delivering parcels to send notifications to customers when a parcel arrives seems less controversial at first sight. It can become controversial, however, if the van movement measuring can be used to instruct, e.g. when an employee is allowed to take toilet or lunch breaks (Schafheitle et al., 2020). Adding to this, in a workplace setting, privacy protection stands in tension with the power relationship between employer and employee, and the potential drawbacks of a consent-based approach, as discussed earlier – employees should not be forced to waive away their privacy rights in exchange for work (Ajunwa et al., 2017).

Anchoring Privacy Due Diligence in business practice – Reporting, evaluating, learning. To anchor Privacy Due Diligence into business practice, management needs to find a way to make the continuous reporting, evaluation and learning about the privacy impacts of its business matter within the company. For example, are there dedicated mechanisms for accountability and oversight for workplace monitoring in consultation with affected stakeholders? Diverse membership and composition in accountability governance structures with a clear, transparent process is key – with an emphasis on taking the view of potentially marginalized voices into account. Key elements could entail measures such as a policy commitment at the highest level, setting out a company's privacy standards, awareness raising measures about data processing practices, or grievance mechanisms for employees and workers to speak out against intrusive measures. The UNGPs suggest operational grievance mechanisms to be accessible directly to stakeholders who may be adversely impacted. Anchoring Privacy Due Diligence in business practice should involve the integration of preventive and remedial mechanisms to act against adverse privacy impacts. The remedial rights to data subjects required by the GDPR can deliver complementarity (see GDPR, Arts. 15, 16, 17, 18, 20). A feedback loop should ensure learning from past mistakes and improve privacy conduct: The management needs to continuously evaluate accountability mechanisms, based on robust stakeholder engagement, rather than doing a static one-time assessment. The individuals conducting the review need to be empowered to change the data models and particular algorithmic decisions, and indeed do so on a regular basis, if needed. Through such structural measures, the management takes ownership of arising privacy dilemma, rather than 'outsourcing' it to the data protection officers. Such management ownership to deal with privacy issues pays justice to the increasing threats posed to privacy in a data-driven workplace.

Conclusion

In this article, we set out to explore the promises of a B&HR approach to tackle the privacy challenges brought on by the rise of algorithmic management. Our review of different legal and technical approaches tackling these challenges revealed a number of promising avenues, but also significant gaps. Despite its popularity in industry circles, for example, design-based approaches do not suffice to protect employees' privacy at the workplace. Legal approaches also fall short, notably given the difficulty of applying jurisdiction-specific norms to a truly global phenomenon.

Privacy Due Diligence vows to play a fruitful role in closing these gaps. The balancing exercise between managerial prerogative and worker protection required by employment law and data protection law cannot be appropriately carried out through tech solutions alone

– nor is *ex post facto* litigation an effective strategy for preventing harms.

Interests need to be weighed before intrusive surveillance begins, and continue to be scrutinized over the course of the data life cycle. By building on existing models of corporate due diligence processes, in combination with key insights from data protection, legal frameworks and ethical considerations, the Privacy Due Diligence model establishes a company-wide process for responsible business conduct towards privacy at work.

Acknowledgements

We would like to thank Gabriel Kasper for useful discussions, and the Swiss National Science Foundation, and Economic and Social Research Council (UKRI) for their support.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This article is partly funded by a grant of the Swiss National Science Foundation, NFP 75 "Big Brother or Big Data"? HR control practices and employee trust, and a grant by the Economic and Social Research Council (UKRI).

ORCID iD

Isabel Ebert https://orcid.org/0000-0001-9080-4210

References

Ajunwa I (2020) The "black box" at work. *Big Data & Society*, October. DOI: 10.1177/2053951720938093

Ajunwa I, Crawford K and Ford (2016) Health and big data: An ethical framework for health information collection by corporate wellness programs. *The Journal of Law, Medicine & Ethics: A Journal of the American Society of Law, Medicine & Ethics* 44: 474–480.

Ajunwa I, Crawford K and Schultz J (2017) Limitless worker surveillance. *California Law Review* 105: 735–776.

Alston P (ed.) (2005) *Non-State Actors and Human Rights*. Oxford: Oxford University Press.

Astor M (2017) Microchip implants for employees? One company says yes. *The New York Times*, 25 July. Available at: https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html (accessed 17 March 2021).

Ball K (2010) Workplace surveillance: An overview. *Labor History* 51(1): 87–106.

Bărbulescu vs. Romania (5 September 2017) App. No. 61496/08 ECtHR.

Bhave DP, Teo LH and Dalal RS (2019) Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management* 46(1): 127–164.

Boyd D and Crawford K (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662–679.

Bradford A (2020) *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Brassart Olsen C (2020) To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR. *International Data Privacy Law* 10(3): 236–252.

Buolamwini J and Gebru T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. *Conference on Fairness, Accountability and Transparency* 81: 77–91.

Bygrave L (2017) Data protection by design and by default: Deciphering the EU's legislative requirements. *Oslo Law Review* 4(2): 105–120.

Bygrave L (2020) The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects. *Computer Law & Security Review* 40: 105460.

California Consumer Privacy Act (2018) AB-375, 13 September.

Cascio WF and Montealegre R (2016) How technology is changing work and organizations. *Annual Review of Organizational Psychology and Organizational Behavior* 3: 349–375.

Cavoukian A (2012) PbD: Origins, meaning, and prospects for assuring privacy and trust in the information era. In: Yee GOM (ed.) Privacy Protection Measures and Technologies in Business Organizations: aspects and Standards. Hershey, PA: IGI Global, pp.170–208.

Cheekoty S (2019) Leveraging workforce analytics using deep learning. *Towards Data Science,* 23 October. Available at: https://towardsdatascience.com/leveraging-workforce-analytics-using-deep-learning-b13427f674bf (accessed 17 March 2021).

Christl W (2017) Corporate surveillance in everyday life: How companies collect, combine, analyze, trade and use personal data on billions. Report, Cracked Labs, Vienna, June.

Collins P (2020) The Right to Privacy, surveillance-by-software and the "Home-Workplace". In: UK Labour Law Blog, 3 September. Available at: https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/ (accessed 17 March 2021).

Council of Europe (2020) Ad Hoc Committee on Artificial Intelligence – Feasibility study, 17 December. Available at: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da (accessed 17 March 2021).

Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, January. Available at: https://rm.coe.int/1680078b37 (accessed 17 March 2021).

Council of Europe (1953) European Convention on Human Rights, as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Strasbourg. Available at: https://www.echr.coe.int/documents/convention_eng.pdf (accessed 17 March 2021).

Council of Europe (2015) Recommendation CM/Rec (2015) 6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet, Strasbourg. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID = 09000016805c3f7a (accessed 17 March 2021).

Council of Europe (1989) Recommendation No. R (89) 2 on the protection of personal data used for employment purposes, 18 January, Strasbourg. Available at: https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf (accessed 17 March 2021).

Cukier K and Mayer-Schoenberger V (2013) The rise of big data: How it's changing the way we think about the world. *Foreign Affairs* 92(3): 28–41.

Dix A (2010) Built-in privacy – No panacea, but a necessary condition for effective privacy protection. *Identity in the Information Society* 3: 257–265.

Ebert I, Busch T and Wettstein F (2020) *Business and Human Rights in the Data Economy. Business and Human Rights in the Data Economy. A Mapping and Research Study*. Berlin: German Institute for Human Rights.

EU Charter of Fundamental Rights (2012) C 326/02, Brussels, October. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri = CELEX:12012P/TXT&from = EN (accessed 17 March 2021).

EU General Data Protection Regulation (GDPR): 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 2016 L 119/1.

European Parliament (2014): Position Recitals 71a and 71b, Art. 23 para, 1, Art. 33 para. 3 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels. Available at: https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_EN.html (accessed 17 March 2021).

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.

European Union Agency for Fundamental Rights (2018) *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, May.

European Union Article 29 Working Party (2002) Guidelines on 2016/679, WP251, 3 October 2017; WP251rev.01, revised 6 February 2018;WP 248 rev.01, revised 4 October 2017; WP 48, 13 September 200; WP 136, 20 June 2007; WP 249, 8 June 2017; WP55, May.

Felzmann H, Fosch Villaronga E and Lutz C (2019) Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society* 6(1). DOI: 10.1177/2053951719860542

Finlay S (2014) *Predictive Analytics, Data Mining and Big Data. Myths, Misconceptions and Methods*. Hampshire: Palgrave Macmillan UK.

Frantziou E (2020) The right to privacy while working from home ('WFH'): Why employee monitoring infringes Art 8 ECHR. In: UK Labour Law Blog, 5 October. Available at: https://uklabourlawblog.com/2020/10/05/the-right-to-privacy-while-working-from-home-wfh-why-employee-monitoring-infringes-art-8-echr-by-eleni-frantziou/ (accessed 17 March 2021).

Grabenwarter C (ed.) (2014) *European Convention on Human Rights: Commentary*. Munich: CH Beck.

Guild E (2019) Data rights: Claiming privacy rights through international institutions. In: Bigo D, Isin E and Rupper E (eds) Data Politics – Worlds, Subjects, Rights. London: Routledge, pp.267–284.

Hartzog W (2018) *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge: Harvard University Press.

Hartzog W and Stutzman F (2013) Obscurity by design. *Washington Law Review* 88: 385–418.

Heaven WD (2020) This startup is using AI to give workers a "productivity score". *MIT Technology Review*, 4 June. Available at: https://www.technologyreview.com/2020/06/04/1002671/startup-ai-workers-productivity-score-bias-machine-learning-business-covid/ (accessed 17 March 2021).

Hillmann L (2015) Mental health issues and the duty to protect workers from risks to their mental health. *Clayton Utz*. Available at: https://www.claytonutz.com/knowledge/2015/august/mental-health-issues-and-the-duty-to-protect-workers-from-risks-to-their-mental-health (accessed 17 March 2021).

Hong R (2016) Soft skills and hard numbers: Gender discourse in human resources. *Big Data & Society* 3(2). DOI: 10.1177/2053951716674237

I v. Finland (17 July 2008) App. No. 20511/03 ECtHR.

International Labour Organization (1997) Protection of workers' personal data. ILO Code of Practice, Geneva, January. Available at: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_107797/lang–en/index.htm (accessed 17 March 2021).

Kälin W and Künzli J (eds) (2019) *Universeller Menschenrechtsschutz*. Basel: Helbing Lichtenhahn Verlag.

Keats Citron D and Pasquale F (2014) The scored society: Due process for automated predictions. *Washington Law Review* 89(1): 1–33.

Kellogg KC, Valentine MA and Christin A (2020) Algorithms at work: The new contested terrain of control. *Academy of Management Annals* 14(1): 366–410.

Koops B and Leenes R (2014) Privacy regulation cannot be hardcoded. A critical comment on the 'PbD' provision in data-protection law. *International Review of Law, Computers & Technology* 28(2): 159–171.

Köpke vs. Germany (5 October 2010) App. No. 420/07 ECtHR.

Kroener I and Wright D (2014) A strategy for operationalizing PbD. *The Information Society* 30(5): 355–365.

Kroll JA, Huey J, Barocas S, et al. (2017) Accountable algorithms. *University of Pennsylvania Law Review* 165: 633–705.

López Ribalda and others vs. Spain, nos. 1874/13 and 8567/13 ECtHR (17 October 2019).

Martini M (2018) Art. 25 DSGVO. In: Paal BP and Pauly D (eds) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar. 2nd ed. Munich: CH Beck Verlag, pp.317–338.

Mateescu A and Nguyen A (2019) Explainer: Algorithmic management in the workplace. *Data & Society*. Available at: https://datasociety.net/output/explainer-algorithmic-management-in-the-workplace/ (accessed 17 March 2021).

McCorquodale R, Smit L, Neely S, et al. (2017) Human rights due diligence in law and practice: Good practices and challenges for business enterprises. *Business and Human Rights Journal* 2(2): 195–224.

McQuay T and Cavoukian A (2010) A pragmatic approach to privacy risk optimization: PbD for business practices. *Identity in the Information Society* 3(2): 379–396.

Mittelstadt BD, Allo P, Taddeo M, et al. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society* 3(2). DOI: 10.1177/2053951716679679

Monahan T (2016) Built to lie: Investigating technologies of deception, surveillance, and control. *The Information Society* 32(4): 229–240.

Montjoye Y, Hidalgo C, Verleysen M, et al. (2013) Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports* 3: 1376. https://doi.org/10.1038/srep01376

Morris S, Griffin D and Gower P (2017) Barclays puts in sensors to see which bankers are at their desks. *Bloomberg*, 18 August. Available at: https://www.bloomberg.com/news/articles/2017-08-18/barclays-puts-in-sensors-to-see-which-bankers-are-at-their-desks (accessed 17 March 2021).

Nagy P and Neff G (2015) Imagined affordance: Reconstructing a keyword for communication theory. *Social Media + Society* 1(2). DOI: 10.1177/2056305115603385

Neff G, McGrath M and Prakash N (2020) AI @ Work – Artificial intelligence in the workplace, August 2020. Available at: https://www.futuresays.org/empower-workers/ (accessed 17 March 2021).

Neff G and Nafus D (2016) *Self-tracking*. Cambridge, MA: MIT Press.

Niemitz v. Germany (1992) App. No. 13710/88 ECtHR, 16 December.

OHCHR B-Tech (2021) Foundational papers. Available at: https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx (accessed 17 March 2021).

Otto M (2019) "Workforce analytics" v fundamental rights protection in the EU in the age of big data. *Comparative Labor Law and Policy Journal* 40: 389–404.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Peterson H (2020) Whole foods tracks unionization risk with heat map. *Business Insider*, 20 April. Available at: https://www.businessinsider.com/whole-foods-tracks-unionization-risk-with-heat-map-2020-1 (accessed 17 March 2021).

Phan P, Wright M and Lee SH (2017) Of robots, artificial intelligence, and work. *Academy of Management Perspectives* 31(4): 253–255.

Prassl J (2018) *Humans as a Service: The Promise and Perils of Work in the Gig Economy*. Oxford: Oxford University Press.

Prassl J (2019) What if your boss was an algorithm? Economic incentives, legal challenges, and the rise of artificial intelligence at work. *Comparative Labor Law and Policy Journal* 41(1): 123.

Rocher L, Hendrickx J and Montjoye Y (2019) Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications* 10: 3069. https://doi.org/10.1038/s41467-019-10933-3

Rubinstein IS (2011) Regulating PbD. *Berkeley Technology Law Journal* 26(3): 1409–1456.

Rubinstein IS (2012) Big data: The end of privacy or a new beginning? *International Data Privacy Law* 3(2): 74–87.

Rubinstein IS and Good N (2013) PbD: a counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal* 28(2): 1333–1413.

Ruggie JG (2007) Business and human rights: The evolving international agenda. *American Journal of International Law* 101(4): 819–840.

Ruggie JG (2013) *Just Business: Multinational Corporations and Human Rights*. New York, NY: WW Norton & Company.

Schafheitle SD, Weibel A, Ebert I, et al. (2020) No stone left unturned? Towards a framework for the impact of datafication technologies on organizational control. *Academy of Management Discoveries* 6(3). DOI: 10.5465/amd.2019.0002

Simitis S (1999) Reconsidering the premises of labour law: Prolegomena to an EU regulation on the protection of employees' personal data. *European Law Journal* 5(1): 45–62.

Singer N (2019) What does California's New Data Privacy Law mean? Nobody agrees. *New York Times*, 29 December. Available at: https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html (accessed 17 March 2021).

Smuha N (2020) Beyond a human rights-based approach to AI governance: Promise, pitfalls, plea. *Philosophy & Technology* 33: 1–14. https://doi.org/10.1007/s13347-020-00403-w

Spiekermann S (2012) The challenges of PbD. *Communications of the ACM* 55(7): 38–40.

Steele C (2020) The quantified employee: How companies use Tech to track workers. *PC Mag,* 14 February. Available at: https://uk.pcmag.com/security-5/124891/the-quantified-employee-how-companies-use-tech-to-track-workers (accessed 17 March 2021).

Tamò-Larrieux A (2018) *Designing for Privacy and Its Legal Framework*. Zurich: Springer.

Thomas LM (2019) Brazil's new privacy law one year away. *The National Law Review*, 21 August. Available at: https://www.natlawreview.com/article/brazil-s-new-privacy-law-one-year-away (accessed 17 March 2021).

Trade Union Congress (2018) I'll be watching you – A report on workplace monitoring. Available at: https://www.tuc.org.uk/sites/default/files/surveillancereport.pdf (accessed 17 March 2021).

United Nations Human Rights Council (2011) *UN Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. United Nations Human Rights Office of the High Commissioner, New York and Geneva.

Ustek-Spilda F, Powell A and Nemorin S (2019) Engaging with ethics in internet of things: Imaginaries in the social milieu of technology developers. *Big Data & Society* 6(2). DOI: 10.1177/2053951719879468

Vincent J (2020) Amazon deploys AI distance assistants to notify warehouse workers if they get too close. *The Verge*, 16 June. Available at: https://www.theverge.com/platform/amp/2020/6/16/21292669/ (accessed 17 March 2021).

Waddell K (2016) The algorithms that tell bosses how employees are feeling. *The Atlantic,* 29 September. Available at: https://www.theatlantic.com/technology/archive/2016/09/the-algorithms-that-tell-bosses-how-employees-feel/502064/ (accessed 17 March 2021).

Wagner B (2018) Ethics as an escape from regulation: From ethics-washing to ethics-shopping? In: Hildebrandt M (ed.) Being Profiling. Cogitas Ergo Sum. Amsterdam: Amsterdam University Press, pp.84–89.

Wagner B (2019) Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems. *Policy & Internet* 11(1): 104–122.

Wettstein F (2015) Normativity, ethics, and the UN guiding principles on business and human rights: A critical assessment. *Journal of Human Rights* 14(2): 162–182.

Wettstein F (2016) From side show to main act: Can business and human rights save corporate responsibility? In: Baumann-Pauly D and Nolan J (eds) Business and Human Rights: From Principles to Practice. London: Routledge, pp.77–87.

Youngdahl J (2009) Solidarity first: Labor rights are not the same as human rights. *New Labor Forum* 18(1): 30–37.