Worker Privacy in a Digitalized World under European Law

Custers, B.H.M.; Ursic, H.

WORKER PRIVACY IN A DIGITALIZED WORLD UNDER EUROPEAN LAW

Bart Custers† and Helena Ursic††

I. INTRODUCTION

In recent years, knowing the people that work for you has certainly become easier for employers. The digitalization and robotization of the workplace has widely exposed employees' data, for instance, on their performance, the number of breaks they take, and the ways in which they cooperate with others. With the exponential growth of social media, the quantified self movement and ubiquitous video cameras, there is little left to anonymity. Together with the shift toward flexible, non-permanent, and less certain employment practices, this means that modern employees are increasingly pushed into an unfavorable position.

Robotization and datafication of work have also had another, perhaps even more important consequence for individual privacy: the private sphere and the sphere of work are increasingly overlapping. Increasing numbers of (white-collar) employees are provided with mobile phones, laptops, and leased cars by their employers, together with remote log-in accounts for working from home or other locations, blurring the lines between what is private and what is work. All kinds of explicit and implicit assumptions (both from employers and employees) regarding an employee's availability for work outside the office and beyond regular working hours erase the once-clear boundaries between the private sphere and the sphere of work, both in location and time. For practical reasons, many employees end up also using mobile phones, laptops, and leased cars provided by their employer for private reasons, either incidentally or structurally. The same goes for email addresses and social media accounts. The same addresses and accounts can be used for both private and work-related communications. What someone posts on Twitter or Facebook can be both a private matter and information

† Associate professor and director of research, eLaw—Center for Law and Digital Technologies, Leiden University, the Netherlands.

†† Resident fellow, Yale Law School (Information Society Project), PhD candidate, Leiden University, the Netherlands.

that concerns work. There is no longer a clear line between what is office and what is home.[1]

Even when employees try to keep strict boundaries between their work and their private life, private information may be accessible for their employers. For instance, when people tell their friends via social media about a long, hard day at work, an argument they had with their boss, or a nasty complaint of a customer, such information may be viewed by others, sometimes including the employers or others who are mentioned in such messages.[2]

All this information may be very useful for employers to gain further insight in their employees, for instance, when hiring new employees or when assessing performance of individual employees. Such individual assessments can now be based on much more information, including information from the private sphere of workers, and much faster and cheaper. It may reveal that John Doe, a prospective employee with excellent background qualifications, is also a party animal outside working hours or has political views that significantly differ from the company policies. Despite his excellent qualifications, John might be rejected for the vacancy because the employer may expect trouble.[3]

In the era of big data, this has been taken to the next level, in which the increased amounts of available information allow for new types of analyses that may reveal novel, unexpected patterns and profiles.[4] Hypothetically, the data might reveal that people who are driving blue cars are the most reliable workers or that singles have the best work performance. All such characteristics and expectations can be ascribed to groups and individuals, obviously affecting the ways in which they are viewed by employers.

The analysis of the data may also yield predictive results. For instance, even when an employee does not share any information on substance abuse or his political or sexual preferences, this information may still be predicted on the basis of Facebook likes.[5] Also, predictions can be made about the

[1] Some regulators consider this blurred line between home and office a very serious issue that should be regulated by law. Both Germany and France have already passed bills that prohibit employers from contacting their employees via email after 6PM. A.J. Rubin, *France Lets Workers Turn Off, Tune Out and Live Life*, THE NEW YORK TIMES, Jan. 2, 2017, https://www.nytimes.com/2017/01/02/world/europe/france-work-email.html.

[2] ECHR, Case of Bărbulescu v. Romania (application no. 61496/08), Sept. 5, 2017; in this case the employer was able to read the employee's intimate messages sent via his company's account.

[3] Elizabeth Garone, *Can Social Media Get You Fired*, BBC CAPITAL, Nov. 3, 2014, http://www.bbc.com/capital/story/20130626-can-social-media-get-you-fired.

[4] Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof Lecture delivered during the public acceptance of the appointment of professor of Global ICT Law at Tilburg University on Feb. 14, 2014, by Prof. dr. Lokke Moerel, http://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf.

[5] M. Kosinski, D. Stillwell & T. Graepel, Private Traits and Attributes are Predictable from Digital Records of Human Behaviour, *Proceedings of the National Academy of Sciences* (PNAS) (2012), www.pnas.org/content/early/2013/03/06/1218772110.

likelihood that an employee will attract a serious form of cancer or a myocardial infarction within the next five years. Employers may be interested to take such risk assessments into account when making a decision on hiring new employees or promoting employees to core functions in their organization.

In this decision-making process, employers increasingly rely on algorithms, i.e., a series of instructions to process data and to create models and profiles based on historical data.[6] This approach involves two important aspects. First, as algorithms yield only a model or a profile, they are by their nature concise and imprecise descriptions of reality. Second, as they learn from historical data they are only capable of capturing gradual changes, but have difficulties dealing with disruptive changes. As a consequence, mistakes cannot be ruled out. In fact, incorrect algorithmic decisions are spotted quite often, notably in the employment context.[7]

At present, employees may have few ways, or none at all, to address this.[8] Non-disclosure of private information may not be realistic and characteristics and attributes that are not revealed may be predicted anyway.[9] Also, employees may have limited or no insight in which information is available about them, how such information is analyzed, and how the analyses yield decisions about them.[10] For instance, when applicants are rejected for a vacancy, they may not be informed about the fact that a computer reviewed the applicant's CV. Even when they would be informed about this, it may be very hard or impossible to challenge the decision.[11] This raises questions about the privacy of employees, but also about other types of issues, for instance, regarding equality,[12] fair treatment, transparency,[13] and lawfulness of data processing and algorithmic decision-making.[14]

[6] Indre Zliobaite & Bart Custers, Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models, 24 ARTIFICIAL INTELLIGENCE & L. 183, 185 (2016).

[7] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

[8] One legal possibility to challenge algorithmic decisions is the so-called right on explanation that some scholar attribute to the EU General Data Protection Regulation. How and if it could actually apply is not yet clear. *See*, *e.g.*, Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, INTERNATIONAL DATA PRIVACY LAW, https://ssrn.com/abstract=2903469.

[9] Bart Custers, *Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination*, PRIVACY OBSERVATORY MAGAZINE (2012).

[10] FRANK PASQUALE, THE BLACK BOX SOCIETY 6 (2015).

[11] Some ideas on how it would be legally possible to establish a right to challenge AI decisions are discussed in Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR (2017), https://arxiv.org/pdf/1711.00399.pdf.

[12] Barocas & Selbst, *supra* note 7.

[13] Mireille Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era*, DIGITAL ENLIGHTENMENT YEARBOOK 41 (2012).

[14] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C.L. Rev. 93 (2014).

The aim of this contribution is to map privacy and related issues of the digitalized and robotized workplace. In order to provide an overview of the major issues at stake, we present four scenarios in this article that can currently be observed in some modern workplaces. These scenarios concern chip implants, social media assessments of prospective employees, algorithmic assessments of employee performance, and health assessments via wearables. Each of these four scenarios is discussed from a data protection and privacy point of view. We show how the increased use of data and technologies in the workplace challenge some key data protection principles. We particularly focus on three of these principles: the principle of lawfulness, the principle of purpose limitation, and the principle of fairness. While we admit that the analysis of workers' data has a big potential to improve the overall performance of a company, we argue that data protection principles should be adhered to nevertheless. This is important because protection of data and individual privacy is also instrumental to many other rights such as personal liberty, dignity, equality, fairness, and justice. Furthermore, in the long term, insufficiently observing privacy and data protection may erode (minimum levels of) trust between employers and employees. Such trust is necessary for employees to focus on their work (rather than on their safety and their position), which is in turn beneficial for employers.[15]

This contribution is structured as follows. Section II describes four scenarios that are currently transforming privacy of modern workers. Section III further examines data protection law in both the United Staes and the European Union. Section IV provides a legal analysis of these scenarios from the perspective of the three most relevant privacy and data protection principles. Section V provides conclusions.

II. FOUR SCENARIOS

A. Scenario 1: Chip Implants

Identification badges are one of the most common methods of identification of employees when they enter a company's premises, but this may change in the near future. The *New York Times* recently reported that employees at Three Square Market, a technology company in Wisconsin, can now be identified with a single RFID (radio frequency identification) chip.[16] RFID is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic

[15] E.L.O. KEYMOLEN, TRUST ON THE LINE: A PHILOSOPHICAL EXPLORATION OF TRUST IN THE NETWORKED ERA (2016).

[16] Maggie Astor, *Microchip Implants for Employees? One Company Says Yes*, THE NEW YORK TIMES, July 25, 2017, https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html.

spectrum to uniquely identify an object, animal, or person. RFID chips are similar to bar code labels in that they typically work with a corresponding scanner or reader.[17] However, their advantage is that they do not need to be positioned right in front of the reader because they communicate with a reader through radio waves.[18] What is striking about this new type of identification is that it is implemented in employees' bodies. More specifically, a chip the size of a grain of rice is injected between their thumb and index finger.[19]

Thus, RFID chips differ from ID badges in that they are no longer carried around and cannot be forgotten when leaving home. The convenience is obvious. By using the RFID technology various tasks such as swiping into the office building or paying for food in the cafeteria can be accomplished with a wave of the hand.[20] However, there are also some apparent negative consequences. The chip cannot be removed without a medical intervention and therefore not only workplace related moves can be tracked but basically any other move throughout the day, including, for instance, night visits to the toilet (which can be a proxy for employees' health status).

Although the technology is highly privacy invasive, it is expected that it will be widely used, in particular in tech-savvy and less privacy prone environments, such as start-up incubators. For example, early adoption of this technology can be expected in multiple-store workplaces filled with start-up companies to enable easy flow between the floors.[21] In fact, only a couple of days after the technology had been launched, more than fifty out of eighty employees at Three Square's headquarters volunteered to it.

B. Scenario 2: Assessing Candidates Based on Social Media Data

LinkedIn is a business-focused social media platform that has been growing rapidly. In only fourteen years, the company has grown from zero to over 400 million users, meaning that it currently manages a strikingly large amount of personal data.[22] In particular, LinkedIn proves useful for job seekers. To help such users, the platform allows for checking the latest vacancies, inspecting the skills of competing candidates, and communicating with recruiters.[23]

[17] Definition *available at* https://www.techopedia.com/definition/24272/rfid-chip.

[18] *Id.*

[19] Astor, *supra* note 16.

[20] *Id.*

[21] Mentioned by Mary Hildebrand, Lowenstein Sandler LLP, at the IAPP KnowledgeNet meeting in New Jersey on Sept. 14, 2017.

[22] Sean Farrell, *LinkedIn's Rapid 14-year Growth Led to $26.2bn Microsoft Deal*, THE GUARDIAN, June 13, 2016, https://www.theguardian.com/business/2016/jun/13/linkedins-rapid-14-year-growth-led-to-262bn-microsoft-deal.

[23] Some of these services are only available for the Premium users of LinkedIn.

Opening profiles to all sorts of services is something that LinkedIn enables by default. Unless a user changes his privacy settings, her profile is publicly viewable.[24] Although a user always has an option to opt out, it is not likely that everyone is aware of it and capable of effectively changing privacy settings in the mode he or she prefers. Furthermore, a Twitter user recently claimed that LinkedIn's *Rapportive* app revealed his profile regardless of the fact that he had had the visibility turned off.[25] It would be very difficult for a non-technically-skilled user to fix or detect the issue

Due to the (often) public nature of social networks, employers may believe that inspecting the social profiles of prospective candidates can be justified during their recruitment processes.[26] In fact, this is what is happening on a regular basis.[27] For recruiters, LinkedIn is one of the most useful pools of candidates. However, recruiters do not only view candidates' profiles on LinkedIn. Other social networks, such as Facebook, can be even more informative. Contrary to LinkedIn, many of these other networks operate in a different, less formal context, meaning that users tend to reveal more personal information. While this is something that recruiters and future employers might be interested in, such interference would almost always be in conflict with privacy expectations of social media users.[28]

C. Scenario 3: Assessing Workers by Using Algorithms

In recent years, algorithmic tools have become increasingly popular to assess workers and to rank them from the most to the least capable. Deliveroo, a food delivery company, uses an algorithm that compares each courier's performance to its own estimate of how fast they should have been.[29] Those at the end of the list are at risk of getting fired. Cathy O'Neil wrote about U.S. teachers who were evaluated and many of them dismissed based on a score of a rating. [30] It then turned out that the algorithm used flawed metrics and that the teachers who were dismissed were actually doing just fine.[31] The tool evaluated teachers largely on the basis of students' test scores, while ignoring how much the teachers engaged the students, worked

[24] *See* LinkedIn privacy policy, Section 3: https://www.linkedin.com/legal/privacy-policy.

[25] *See also* https://www.reddit.com/r/privacy/comments/3blyrg/linkedin_privacy_violation.

[26] Article 29 Working Party, Opinion 2/2017 on data processing at work, June 8, 2017.

[27] Michael Stephan, David Brown & Robin Erickson, *Talent Acquisition: Enter the Cognitive Recruiter*, 2017 GLOBAL HUMAN CAPITAL TRENDS, Feb. 28, 2017, https://dupress.deloitte.com/dup-us-en/focus/human-capital-trends/2017/predictive-hiring-talent-acquisition.html.

[28] Bart Custers, Simone van der Hof & Bart Schermer, *Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies*, 6 POL'Y & INTERNET 268–95 (2014).

[29] Sarah O'Connor, *When Your Boss is an Algorithm*, FINANCIAL TIMES, Sept. 8, 2016, https://www.ft.com/content/88fdc58e-754f-11e6-b60a-de4532d5ea35.

[30] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 41 (2016).

[31] *Id.*

on specific skills, dealt with classroom management, or helped students with personal and family problems.

A similar example that demonstrates how employers not only monitor but also manipulate workers by using big data comes from Uber. Uber is a ride-sharing platform that optimizes the taxi network by introducing greater data intelligence.[32] For commercial reasons, the company wants to keep up the number of available cars, even during times of low demand when drivers make less money. To address this, the company drew on behavioral economic research about the psychological tendency of taxi workers to set round earnings goals and stop working when they reach them.[33] Uber discovered that drivers quickly abandon mental income targets in favor of working at times of high demand.[34] To combat this tendency, Uber sent tailored nudging messages to drivers indicating when they are close to revenue target during times when it was advantageous for Uber to keep its drivers on the road.[35] This was only possible to do on the basis of the analysis of big data that was being instantly collected from all the drivers' mobile devices.

D. Scenario 4: Awarding Bonuses to Employees That Share Their Sport Tracker's Data

In order to encourage employees to be more active, some employers provide reward-based health schemes through which employees compete and collect points that eventually lead to awards and bonuses. These schemes can be composed of several components: a tracking app that employees install on their phones,[36] a health assessment platform that monitors employees' progress[37] and an app that provides daily workouts.[38] Also, access to data generated by wearables that people already use may be granted by employees to employers. For instance, devices such as Fitbit and Jawbone are popular sport trackers that many people already use in private life. Within the quantified self movement,[39] increasing numbers of people incorporate technology into their daily lives to gather data on their food consumption, air quality, moods, physical performance, and physiognomy, including levels of blood oxygen, blood pressure, arousal, and heart rates. The data may also reveal how many hours people spend outdoors, how many hours they sleep,

[32] BART VAN DER SLOOT, DENNIS BROEDERS & ERIK SCHRIJVERS, EXPLORING THE BOUNDARIES OF BIG DATA 27 (2016).

[33] Alex Campolo et al., *AI Now 2017 Report*, AI NOW (Andrew Selbst & Solon Barocas ed., 2017), https://ainowinstitute.org/AI_Now_2017_Report.pdf.

[34] *Id.*

[35] *Id.*

[36] Jiff, app that is commonly used for sport-activity tracking, https://www.jiff.com/privacy.

[37] Corporate health assessment platforms are typically closed from public access.

[38] Example of an app that offers daily workouts, https://7minuteworkout.jnj.com

[39] M. Swan, *The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery*, 1 BIG DATA 85 (2013).

and how much they walk during the day. When devices are connected to the Internet of Things, further information may be disclosed. For instance, electronic toothbrushes may reveal how often and how long people brush their teeth.

While the main point of these reward systems is to take employees' health to a next level, the large amount of data that is collected on the platform and by the apps can give very useful insights to employers. Privacy policies may promise that health-related information will not be disclosed. However, employers may still have access to non-health-related data that is also gathered through apps and websites such as location data. What is more, anonymized data may be shared with third parties. For example, employees' data can be shared with insurance companies. Even though this data cannot identify a single employee it may enable insurers to construct a useful group profile (i.e., a property or a collection of properties of a group of people), which eventually leads to predictions about characteristics of individual employees.[40] In this way, an insurance company may access the information that an employee may not want to (and neither is required to) reveal.

III. DATA PROTECTION LAW

In this section we further examine the applicable data protection law in the European Union, setting the stage for the legal analysis of the scenarios in Section IV. Historically, regulation proceeds from the OECD's guidelines on the protection of Privacy and Transborder Flows of Personal Data, the so-called OECD privacy principles.[41] In Europe, the FIPs are further incorporated in legislation. First, these principles were incorporated in the Council of Europe's 1981 Treaty of Strasbourg.[42] In 1995, the European Union incorporated the FIPs and OECD principles in EU Directive 95/46/EC, the so-called Data Protection Directive (DPD) that is replaced by the General Data Protection Regulation (GDPR) in May 2018. Section III.A provides background information on the contents of the privacy principles and section III.B provides an introduction to the GDPR and its contents.

A. The OECD Privacy Principles

In 1980, a set of principles for fair information processing was developed by the Organization for Economic Co-operation and Development (OECD). The OECD is an organization of thirty-five countries worldwide

[40] BART H.M. CUSTERS, THE POWER OF KNOWLEDGE: ETHICAL, LEGAL, AND TECHNOLOGICAL ASPECTS OF DATA MINING AND GROUP PROFILING IN EPIDEMIOLOGY (2004).

[41] Omar Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1220 (2013).

[42] Council of Europe, Convention No. 108, Jan. 28, 1981. Convention for the protection of individuals with regard to automatic processing of personal data.

(including the United States, Canada and most EU Member States) that is committed to democratic government and a market economy that works on economic and social issues.[43] The principles developed by the OECD, commonly referred to as *the privacy principles*, are [44]

- the *collection limitation principle*, stating that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject";[45]
- the *data quality principle*, stating that "[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date";
- the *purpose specification principle*, stating that "[t]he purposes for which personal data are collected should be specified . . . and that the data may only be used for these purposes";
- the *use limitation principle*, stating that "[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified, . . . except a) with the consent of the data subject; or b) by the authority of law";
- the *security safeguards principle*, stating that reasonable precautions should be taken against risks of loss, unauthorized access, destruction, et cetera, of personal data;
- the *openness principle*, stating that the subject should be able to know about the existence and nature of personal data, its purpose, and the identity of the data controller;
- the *individual participation principle*, stating, among other things, that the data subject should have the right to have his personal data erased, rectified, completed, or amended;
- the *accountability principle*, stating that the data controller should be accountable for complying with measures supporting the above principles.

The first four principles focus on the data and the conditions under which processing of the data is allowed, and the other four principles are duties of those responsible for the processing of personal data and rights of the data subjects. It is important to note that these principles mainly focus on procedural justice, rather than on substantive justice. All these principles are

[43] *See* http://www.oecd.org.

[44] *See* http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

[45] This principle is sometimes referred to as the *principle of minimality*, see L.A. Bygrave, *Data Protection Law; Approaching its Rationale, Logic and Limits*, 10 INFORMATION LAW SERIES 341 (2002).

incorporated in the GDPR and hence binding provisions in the European Union.

B. The EU Legal Framework for Data Protection

The General Data Protection Regulation (GDPR) is an EU regulation, a legislative instrument that is directly binding for all EU Member States and its citizens.[46] It replaces the EU Data Protection Directive of 1995, a legislative instrument that needed to be implemented in national legislation by each EU Member State. To a large extent, the directive carried over the OECD idea of a set of fundamental data protection principles. In essence, the GDPR builds on the provisions in the EU Directive it replaces, but further strengthens, several data subject rights (such as the right to data portability and the right to be forgotten)[47] and introduces some new concepts (such as data protection impact assessments, privacy by design and data breach notifications).[48]

The scope of the GDPR is on personal data, which is defined in article 4.1 as any information relating to an identified or identifiable natural person (the data subject). This excludes anonymous data and data relating to legal persons. Data on deceased people is not personal data and therefore beyond the scope of the GDPR.[49] For collecting and processing personal data, there are several provisions that data controllers have to take into account. First of all, all processing has to be lawful, fair, and transparent (art. 5.1). Furthermore, the purposes for which the data are collected and processed have to be stated in advance (purpose specification) and the data may not be used for other purposes (purpose or use limitation) and data may only be collected and processed when necessary for these purposes (collection limitation or data minimization). Data has to be accurate and up-to-date (data quality). When data is no longer necessary, it has to be removed (storage limitation). The data needs to be processed in a way that ensures appropriate security and has to be protected against unlawful processing, accidental loss, destruction, and damage (data integrity, confidentiality). Furthermore, the data controller is responsible for compliance (accountability, art. 5.2).

Processing is only lawful when the data subject has given consent, when the processing of the data is necessary for the performance of a contract, when the processing is necessary for compliance with a legal obligation (usually for law enforcement purposes) or any of the other legal bases

[46] European Parliament and Council Regulation (EU) 2016/679 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) [2016] OJ L 119.

[47] *See* Chapter 3 of the GDPR.

[48] *See* Chapter 4 of the GDPR.

[49] E. Harbinja, *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?*, 10 SCRIPTED 19 (2013).

provided in article 6. This list of legal bases is exhaustive: when none of them applies, the collecting and processing of personal data is not allowed. The processing of sensitive data such as personal data revealing ethnicity, political or religious beliefs, genetic data, or data concerning sexual orientation is not allowed, unless exceptions apply (art. 9).

Data subjects have several rights regarding their personal data, including a right to transparent information on the data collected and the purposes for which it is processed (art. 12–14), a right to access to their data (art. 15), a right to rectification (art. 16), a right to erasure (art. 17), a right to data portability (art. 20), and a right not to be subject to automated decision-making (art. 22).

IV. Legal Analysis

The four scenarios show that ubiquitous data processing has become a reality of the modern workplace. The use of employees' data leads to streamlined and more efficient processes.[50] Modern data analytics saves time and resources, and it helps workers keep healthy bodies and sane minds. However, any data processing of personal data, regardless of how technologically developed or commercially needed it is, has to comply with a number of data protection principles. With the adoption of the new General Data Protection Regulation (GDPR), these principles have been strengthened and detailed.[51] Although modern data processing gives an impression that it could escape strict data protection rules, this should not be the case. The "old" privacy principles should apply to all types of use of personal data in a modern workplace.[52] That said, we observe that the widespread use of data puts many of these principles under pressure. In what follows, we specifically discuss three of them: the principle of lawfulness (Article 6 of the GDPR), the principle of fairness (Article 5(1)(a) of the GDPR), and the principle of purpose limitation (Article 5(1)(b) of the GDPR).

A. The Principle of Lawfulness

The principle of lawfulness is not one of the original OECD privacy principles. It is introduced in EU legislation as the principle that states that

[50] *See* https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/using-people-analytics-to-drive-business-performance-a-case-study.

[51] Christopher Kuner, *The EuropeanCommission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, 9 PRIVACY & SECURITY LAW REPORT (2012), http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf.

[52] European Data Protection Supervisor, Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, 14 (2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

all data processing should be based on a solid legal basis. The GDPR gives an exhaustive list of options: consent, contract, legitimate interest, legal provision, vital interest, and public interest. As mentioned above, in case none of these options apply, the processing of personal data is illegal. In the context of employment, the first three are particularly relevant.

To start with, data processing may be based on an employment **contract**. Obviously, the processing of an employee's contacts, financials and his family members' data is critical for an employer to perform the contract, i.e., to fulfill their obligations such as paying the salary and providing other sorts of remuneration. However, the employment contract can only work as a legal basis for the processing of data as long as this processing is necessary for the performance of the contract. In our four scenarios this will most likely not be the case as for none of them the use of data is indispensable for performing the contractual obligations.

An alternative legal basis to justify data processing in the context of employment is a data subject's **consent**. Consent is a fundamental concept in privacy and personal data protection and often used as the legal basis for the processing of personal data.[53] When people agree to the use of their personal data, it makes any discussing about lawfulness of data collection and processing more or less obsolete. However, there are many issues with consent. For instance, any consent decision has to be independent in order to be valid. In labor relations, this can be complicated because people may need their jobs to make a living. Employees may think the chip implants in Scenario 1 may "come with the job" and feel pressure that refusal may result in not getting hired for a job or as a career-limiting move. Also the technology may limit the options to choose from, disallowing partial consent. For instance, the chip implants in Scenario 1 may be acceptable for employees during working hours, but not during their private life. However, the design of the technology does not allow for turning the chips on and off.

In order to be valid, consent has to be informed consent.[54] Obviously, people have to receive some information about what they do or do not consent to, otherwise consent mechanisms make no sense. However, providing such background information may be complicated, also, in the four scenarios described in this article. Research shows that from privacy policies it is often not clear to people what data is collected, for what purposes, how the data is analyzed, and which decisions result from the analyses.[55] Also, it may not be clear who can be held accountable and how to exercise rights. Furthermore,

[53] Consent remains a fundamental concept for data protection law under the GDPR as well (regardless all the criticism). Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 79 (2013).

[54] Custers, van der Hof & Schermer, *supra* note 28.

[55] D.J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880–1903 (2013).

consent can easily be bypassed. For instance, when people put information about others on social media ("today my friend admitted she has a horrible boss and is looking for a new job"), it may be without consent of the person the data concerns. In the United States, publicly available information is beyond privacy protection.[56] In the European Union, such data in principle cannot be used by employers, but this may be difficult to enforce.

People may be unable to overview the consequences of consent decisions.[57] For instance, consenting to the use of sport tracker's data (Scenario 4) by employers may look interesting for both employees and employers as they both benefit from good health and health conditions. However, when the data unexpectedly reveals that the employee is very likely to attract a serious disease in the next few years, this may affect his job, health insurance, and quality of life in ways that may be difficult to foresee. In some cases, particularly when no cure or therapy exists, people may prefer not to know such information.[58] Short term benefits, like bonuses, may be difficult to balance against long term concerns.

Concerns around the legal feasibility of consent have led EU authorities to consider a move from the legal basis of consent to the legal basis of **legitimate interest**.[59] On these grounds, employers can process their employees' data when their commercial interest are so strong that they prevail over employees' rights such as privacy, data protection, etc.[60] This will not easily be the case, but may be legal basis for data processing in some cases. For instance, the U.K. Information Commissioner's Office explicitly called for moving from consent to an alternative basis: "If you are processing employee data . . . you should look for another basis for processing such as 'legitimate interests.'"[61] Similarly, the Centre for Information Policy Leadership has argued strongly in favor of using legitimate interest as a legal basis that fits best to the new technologically-driven environment.[62] Possible situations in which legitimate interest could be used are extremely broad,

[56] The so-called third-party doctrine. Although this legal concept has been recently challenged—see Sotomayer's concurring opinion in United States v. Jones, 132 S.Ct. 945 (2012). Stephen E. Henderson, *After* US v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431 (2013).

[57] Bart Custers et al., *Informed Consent in Social Media Use: The Gap between User Expectations and EU Personal Data Protection Law*, 10 SCRIPT-ED 435–457 (2013).

[58] THE RIGHT TO KNOW AND THE RIGHT NOT TO KNOW: GENETIC PRIVACY AND RESPONSIBILITY (Ruth Chadwick, Mairi Levitt & Darren Shickle 1997).

[59] *See*, *e.g.*, Article 29 Working Party, *Opetion 2/2017 on Data Processing at Work*, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

[60] *Id.*

[61] Debbie Heywood, *Lawful Processing of HR Data Under the GDPR*, TAYLOR WESSING, Mar. 2017, https://www.taylorwessing.com/globaldatahub/article-processing-of-hr-data-under-the-gdpr.html

[62] Centre for Information Policy Leadership, Recommendations for Implementing Transparency, Consent and Legitimate Interest Under the GDPR, (2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/06/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

ranging from background checks and security vetting in recruitment and HR functions, office access and operation, professional learning and development administration, travel administration, time recording and reporting, to processing of family members' data in the context of HR records. Basically, any of the scenarios presented in Section 2 could fit one of these categories. However, legitimate interest should not be a "carte blanche." It should be made specific, respect privacy expectations of employees and be supported with privacy-friendly design.[63] In particular, the use of pseudonymous data was recommended as the optimal safeguard.[64]

In an opinion from 2014, the Article 29 Working Party, an EU data protection advisory body consisting of representatives of national data protection authorities, confirmed that the notion of legitimate interest could indeed include a broad range of interests, however, these interests will always have to be balanced against the interests and fundamental rights of the data subjects.[65] This second step requires a more strict and substantive analysis that may be a pain in the neck for employees who want to introduce technological developments that cannot be described as something strictly necessary. For example, how would an employer argue that inserting chips in employees' hands (Scenario 1) is a very urgent measure that prevails over employees' fundamental rights to privacy, health, dignity, etc.?

In addition to requiring a balancing of rights, which is never clear-cut, legitimate interest as a legal basis can be dangerous as it rules out data subject control. Do and should employees trust employers to take care of their rights and to conduct the balancing test in a way that strikes a fair balance? As the European Court of Human Rights noted in *Bărbulescu v. Romania*, a too-relaxed dealing with employee data may erode the trust between employees and employers.[66] Employees may be skeptical about the results of the balancing. For example, in Scenario 3, in which the processing of data in order to assess a worker's performance may lead to very serious consequences for someone's social and financial security. One legal safeguard in the GDPR is the right to object (Article 21) but not everyone may be aware of this right and/or willing to actually apply it. Also, the right is limited in scope since the employer may demonstrate "compelling reasons" that override the objection.

The problem of choosing the right legal basis has also revolved around the upcoming e-Privacy regulation, a *lex specialis*, which aims at protecting

[63] *Id.*

[64] Gwendal Le Grand, Jules Polonetsky & Gary LaFever, GDPR Data Analytics Webinar Summary Three Key Points.

[65] Article 29, Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directived 95/46/EC, *available at* http://www.dataprotection.ro/servlet/ViewDocument?id=1086.

[66] Case of Bărbulescu v. Romania, (Application No. 61496/08), ¶ 121.

electronic communication data. This data can be highly sensitive, especially in the workplace. A typical example are personal emails, telephone calls and instant messages (e.g., via WhatsApp), which now also fall under the scope of e-Privacy law. Some commentators of the draft regulation have argued against introducing the basis of legitimate interest for the processing of communication data.[67] In a specific regime, such as the ePrivacy regime, there is less need for open norms.[68] Adding to that the distinct nature of the employment relationship, the argument becomes even stronger. For the reasons explained above, consent may not be a useful legal basis in the employment context either. However, in the employment relationship, there will certainly be some situations in which processing of personal data is needed and legitimate. One example may be when an employer offers employees the ability to lease cars and for administrative purposes lets a third party collect location data via the onboard unit of a car.[69] If neither legitimate interest nor consent can be used to justify the processing, should employers abandon the idea of sharing data with the car leasing company? To solve this problem, it has been suggested that the general prohibition of consenting to an interference with an employee's terminal equipment (i.e., onboard unit) should include an exception that would apply in some limited cases.[70]

B. Principle of Purpose Limitation and Specification

Both the legal basis of consent and the legal basis of legitimate interest are limited in the sense that they can only justify one specific and limited type of data processing. This is because of the principle of purpose limitation, which stipulates that data must be collected for a specified, explicit, and legitimate purpose and must not be further processed in a way incompatible with those purposes.[71] If an employer decides that data should be processed for a new purpose after a while, say to perform yet another assessment of efficiency of the workers, in principle renewed consent should be asked for or a new balancing of the interests should be conducted. One important reason behind the purpose of data processing is that any use of data should remain within a data subject's reasonable expectations.[72] However, this can be difficult in a modern workplace.

The increase in the amount of data generated by and about employees, in combination with new techniques for data analysis and cross-matching,

[67] Frederik Zuiderveen Borgesius et al., An Assessment of the Commission's Proposal on Privacy and Electronic Communications 65 (2017), https://www.ivir.nl/publicaties/download/IPOL_STU2017 583152_EN.pdf.

[68] *Id.*

[69] *Id.* at 65.

[70] *Id.*

[71] GDPR, art. 5.

[72] Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, 4 (2013).

create risks of incompatible further processing. This can be illustrated by all four scenarios. In Scenario 2, data chips track location data of employees. However, this data can be used as a proxy for many other types of information. For instance, regular visits to a doctor indicate that an employee may have health issues. In Scenario 2, data scraped from social media, where people typically communicate in a relaxed, informal manner, is reused for the purposes of employees' pre-screening and sometimes for hiring purposes. In Scenario 3, drivers' location data that was collected during the rides, later gave Uber the possibility to manipulate workers in order to keep them on road for a longer time periods. Finally, in Scenario 4 the data flowing from smart devices can be transferred to an insurer and used to assess employees' credit risk.

Although exceeding the purpose limitation is legally banned, it can easily happen in practice. First, employers may fail to specify the reasons for data processing. For example, in Scenario 4, the apps that tracks employees' sport performance often uses an open and vague language. However, as the ECtHR stressed, only specific reasons can justify the introduction of the monitoring measures.[73] Second, employers may hide secondary purposes in long, legalistic texts of privacy policies that no one reads. Last, employers may use anonymized data to which data protection law no longer applies. As will be shown in the next subsection, anonymized data is not an innocent source of data either. In some cases, it may negatively affect individuals just like personal data does, leading to discrimination and loss of privacy.

C. Principle of Fairness: Beyond Data Protection

The principle of fairness is, strictly speaking, not one of the OECD privacy principles. Nevertheless, it is rather an overarching principle in data protection law.[74] Adhering to the Fair Information Practices, the OECD privacy principles, and/or EU data protection law should ensure fairness regarding the processing of personal data. In fact, EU data protection law contains a principle on fairness that is linked with numerous procedural safeguards that should, as a whole, constitute fair processing of data.[75] However, it should be noted that this focuses on procedural fairness rather than substantive fairness. In fact, companies can be entirely compliant with EU data protection law, and still people may perceive interference with their privacy—the so-called privacy paradox.[76] The analysis of the principles of

[73] Supra 66.

[74] Damian Clifford & Jef Ausloos, *Data Protectiona nd the Role of Fairness* (CiTiP Working Paper Series, 2017).

[75] *Id.*

[76] Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007).

lawfulness and purpose limitation in the sections above has demonstrated that merely adhering to the principles do not necessarily solve the problems. For this reason, we also look beyond privacy and data protection law to examine fairness in a more substantive way. We particularly focus on issues regarding transparency and discrimination.

1. Transparency

Recital 60 of the GDPR explains the meaning of the transparency principle by using a somewhat procedural diction. Transparency requires that *"*any information addressed to the public or to the data subject [is] concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.*"* In the binding text (art. 12) the GDPR takes an even more formalistic approach and constructs transparency as a set of mechanisms and safeguards such as an exemplary list of information that individuals should receive and a possibility to use icons. In the context of employment, the transparency requirement translates into being aware of some key aspects of data processing. Among them are the existence of any monitoring, the purposes for which personal data are to be processed, and any other information necessary to guarantee fair processing.[77]

However, transparency is more than ticking a box and checking if every aspect has been put on the list in a company's privacy policy. Rather, transparency has an important substantial angle that encompasses equality, or, in other words, the *balance of powers*.[78] The developments in the big data economy have led to an imbalance in powers among the actors on the data-driven markets.[79] This is particularly troubling in the context of employment, where an employer typically has much more power over personal data than an employee.[80] Firing a teacher for non-transparent reasons in Scenario 3 has shown what can happen if employees are not aware of the methods used for processing their data and if they cannot challenge possible consequences. Furthermore, non-transparency also negatively affects data subjects in other ways, as shown in Scenarios 2 and 4. In the former case, a law firm might have invited people for interviews after their CVs were ranked by algorithms. Those that did not succeed may never find out what factors the algorithm

[77] Article 29 Working Party, Opinion 2/2017 on data processing at work, June 8, 2017.

[78] *Id.*

[79] Frank A. Pasquale, *Two Narratives of Platform Capitalism*, 35 YALE L. & POL'Y REV. 309 (2016).

[80] Sophie van Bijsterveld, *Transparency in Europe II: Public Access to Documents in the EU and its Member States*, Report From the Conference Hosted by the Netherlands During its Chairmanship of the EU Council, The Hague, Nov. 25–26, 2004, at 65, https://www.bigwobber.nl/wp-content/uploads/2009/01/transparencyineuropeii.pdf.

took into account when making the decision and how their applications were assessed. In the latter case, employers may be linking their fitness trackers to health insurance schemes, offering discounts to those who meet certain goals. What exactly is the performance that leads to rewards and bonuses, is not easy to figure out when the decision is made on a multi-factor and multi-level analysis of workers' data.

The essential problem with transparency in big data and algorithms is that it is difficult to implement.[81] The process of implementation is challenged on two fronts—on the legal and on the practical front. As for the legal, the biggest obstacle is the limited scope of the GDPR provisions.[82] Article 12 and 13 of the GDPR introduce a novel provision on the information about automated decision-making, which could be helpful in ensuring more transparency in the cases of AI-driven analyses. However, since this provision applies to solely automated decisions it could be read as only applying to decisions that involve no human intervention whatsoever.[83] In reality, most decisions will involve at least a minimum of human intervention. In such cases, this specific safeguard will not be applicable anymore.[84] Furthermore, the provision only refers to the information about some general aspects of the automated decision making. In order to guarantee full transparency, an individual would also need the information about the logic behind a specific decision, say his work performance score, and the consequences that he may face, say, a lower salary or getting fired.[85] Unless the courts adopt a very broad interpretation, there is little basis for such transparency in the GDPR.[86]

In practical terms, transparency is difficult to achieve because of the complex nature of algorithmic decision-making. Some types of AI analysis, for instance machine learning, can yield unexpected, novel results that cannot be explained beforehand to data subjects, because they develop gradually, learn from past decisions and therefore become largely unpredictable.[87] What is more, transparency "as a method to see, understand and govern complex systems"—both in the past, and now in the time of algorithmic machine learning systems—is not only limited but sometimes also misleading and even actively unhelpful.[88] Because of this, it has been suggested that the focus should not be on the understanding of the decision-making process, but on

[81] Wachter, Mittelstadt & Floridi, *supra* note 8.

[82] *Id. See also* Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 19 (2017).

[83] Article 22 of the GDPR.

[84] Isak Mendoza & Lee A. Bygrave, The Right Not to Be Subject to Automated Decisions Based on Profiling (Univ. of Oslo Faculty of Law Research Paper No. 2017-20), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855.

[85] Wachter, Mittelstadt & Floridi, *supra* note 8.

[86] Edwards & Veale, *supra* note 81, at 23.

[87] J. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 638 (2017).

[88] Edwards & Veale, *supra* note 81, at 34.

the understanding why a decision has been reached and how it can be challenged.[89]

In addressing these legal and practical restraints, the EU may find some inspiration in the U.S. legal system. Recently, the New York City Council discussed a proposal for an amendment of the city administrative code that would introduce the right to challenge AI decisions.[90] Contrary to the GDPR, it would also make it possible to challenge those more specific decisions. Such an approach can be useful, not only in the context of a smart city, which is where the NYC council's greatest concern lies, but also in the context of employment where AI driven decisions are becoming increasingly common. As a soft law measure, such a mechanism could be implemented by employers to demonstrate their accountability and commitment to fair use of data.

From a technological perspective, the further development and implementation of so-called Transparency Enhancing Technologies (TETs) may be considered.[91] Their function is the anticipation of profiles that may be applied to particular data subjects, possibly constructed out of anonymous data. Providing data subjects with some idea of selection mechanisms that may be applied, allows them adequate anticipation, creating a joint responsibility.[92] For this, a data subject would need access to both his own personal data, the profiling tools and additional external data sources. Based on this information, the data subject could perform a kind of counter profiling.[93] On an individual level, TETs may assist people in making decisions that do not affect their personal score (e.g., credit score, performance rating, etc.). On a mechanism level, scoring procedures that are not sound will likely become less useful and would thus be avoided, limiting the use of algorithms to socially justified ones. On a societal level, public scrutiny may reveal types of scoring that are arbitrary, discriminating or otherwise at odds with societal norms and values. Via the risk of public outrage or reputation damage, social pressure may cause data controllers to abandon abusive profiling practices.[94]

[89] Wachter, Mittelstadt & Russell, *supra* note 11, at 1.

[90] http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0.

[91] Mireille Hildebrandt et al., Behavioural Biometric Profiling and Transparency Enhancing Tools (2009), *available at* https://www.researchgate.net/publication/315786812_Behavioural_biometric_profiling_and_transparency_enhancing_tools.

[92] Anton Vedder & Bart Custers, *Whose Responsibility Is It Anyway? Dealing with the Consequences of New Technologies*, *in* EVALUATING NEW TECHNOLOGIES: METHODOLOGICAL PROBLEMS FOR THE ETHICAL ASSESSMENT OF TECHNOLOGY DEVELOPMENTS 21 (Paul Sollie & Marcus Düwell eds., 2009).

[93] Mireille Hildebrandt & Martin Meints, *RFID, Profiling and AmI*, FIDIS DELIVERABLE 7.7 (2006), *available at* http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf.

[94] Rainer Böhme, *Conformity or Diversity: Social Implications of Transparency in Personal Data Processing*, *in* MANAGING INFORMATION RISK AND THE ECONOMICS OF SECURITY 291 (2008).

2. Discrimination

Obviously, some characteristics are not considered suitable for decision-making. Several particularly sensitive characteristics, such as gender, marital status, ethnicity, and political and religious beliefs, are explicitly prohibited for decision-making in workplaces. The characteristics that are considered unsuitable or illegal may vary a bit from country to country.[95]

Obviously, when sensitive data about employees, either at an individual level or at a group level, is available, it could be used for job related decision-making, such as hiring or firing employees or promotion and bonuses. For instance, employers may prefer hiring men to women or may refuse to promote people from ethnic minorities. Although this is prohibited, it may be difficult to enforce, as people may be unaware of this and even if they are aware, this may be hard to prove.

In the era of big data there is another complicating factor in this, and that is indirect discrimination, also referred to as discrimination by proxy.[96] Analyzing large amounts of data may reveal correlations between sensitive characteristics (such as religion, age, etc.) and trivial, non-sensitive characteristics (such as zip codes, music preferences, etc.).[97] Obviously, these patterns can be used to conceal discrimination, which may happen intentionally (so-called "masking") or unintentionally. For instance, in Scenario 3, when patterns reveal the best teachers work in specific neighborhoods, selecting on the basis of zip codes may inadvertently result in a workforce lacking ethnic diversity.

Also, the information on which profiling and algorithmic decision-making takes place may be biased in the first place.[98] Consider the following example. A company wants to create the ideal profile for their next top manager. On the basis of the data available, the algorithms discover that the ideal top manager is a middle-age white male. It may be obvious that this is a self-fulfilling prophecy: the database probably contained a lot of top managers with this profile and the resulting pattern only confirms what was already expected. When the company actually would use such a profile for their recruitment, it may be argued that they do not give people with different backgrounds (women, people from ethnic minorities, younger, or elderly people) a fair chance. Scenario 4 indicates the same problem—employers

[95] An excellent overview of differences is provided by Daniel Solove, *What Is Sensitive Data? Different Definitions in Privacy Law*, TEACHPRIVACY, July 31, 2014, https://www.teachprivacy.com/sensitive-data-different-definitions-privacy-law.

[96] Anupam Datta et al., Proxy Discrimination in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs 3 (2017), https://arxiv.org/pdf/1707.08120.pdf.

[97] BART CUSTERS, THE POWER OF KNOWLEDGE 19 (2004).

[98] Barocas & Selbst, *supra* note 7.

may link fitness trackers data to health insurance schemes, offering discounts to those who meet certain goals. With a great certainty, the younger employees will probably perform better, which again raises the risk of discrimination.

It is important to note that more accurate data may not solve this problem. Also, removing sensitive data from databases may not avoid the discovery of discriminating patterns.[99] In fact, using such sensitive data in building models may actually better prevent such discriminating patterns.[100]

In addressing the problem of data-driven discrimination, data protection law is probably not the ideal measure. To some extent, privacy-by-design rules could be used to mandate fair design of data analytics tools.[101] In addition, a data ombudsman could be appointed to monitor possibly discriminatory data-driven decision making. The mandate of such an official could be limited to a few problematic areas such as self-driving cars and e-health.[102] Given the challenges that we have explained above, monitoring the use of data in the workplace should also be within the limits of their powers.

V. CONCLUSION

The world is changing and so is the working space. What used to be cubicle walls are now open spaces. What used to be an employee's free time, is now filled with job-related email alerts. In this article, we mapped privacy and related issues of the digitalized and robotized workplace using four scenarios (i.e., chip implants, social media assessments of prospective employees, algorithmic assessments of employee performance, and health assessments via wearables) that can nowadays be observed in some modern workplaces. Using these scenarios, we showed how the increased use of digitalization and robotization in the workplace challenge some key data protection principles, such as the principle of lawfulness, the principle of purpose limitation, and the principle of fairness.

[99] F. Kamiran & T. Calders, *Classifying without Discriminating*, *in* IEEE INTERNATIONAL CONFERENCE ON COMPUTER, CONTROL & COMMUNICATION (2009), http://ieeexplore.ieee.org/document/4909197/?reload=true.

[100] J. Zliobaite & Bart Custers, *Using Sensitive Personal Data May Be Becessary for Avoiding Discrimination in Data-Driven Decision Models*, 24 ARTIFICIAL INTELLIGENCE & L. 183 (2016).

[101] Article 23 of the GDPR; Edwards & Veale, *supra* note 81; PbD could also be a way to more algorithmic accountability, which is described as the use of techniques from computer science to create systems with properties that can be checked by regulators or the public *without revealing the underlying code and data*. Kroll et al., *supra* note 86.

[102] Ian Sample, *Computer Says No: Why Making AIs Fair, Accountable and Transparent is Crucial*, THE GUARDIAN, Nov. 5, 2017, https://www.theguardian.com/science/2017/nov/05/computer-says-no-why-making-ais-fair-accountable-and-transparent-is-crucial.

Regarding the principle of lawfulness, consent is challenged by the mere fact that there is an imbalance between an employer and an employee and it is challenged because of the new types of data processing in which an informed decision is almost impossible to make. The principle of purpose limitation conflicts the very idea of the data economy, which is to reuse data. There is inherent pressure for more efficient use of data that often comes at the expense of employees' privacy. Regarding the principle of fairness, in the workplace more and more decisions are taken automatically with the use of AI tools. These tools lack transparency and are difficult to challenge.

The analysis of workers' data has a big potential to improve the overall performance of a company, but, at the same time, digitalization and robotization have created a very turbulent situation for modern workers. We argue that data protection principles should be adhered to nevertheless. Adapting new technologies and use of data to the sometimes rigid rules of data protection law is not always easy, but it is indispensable because protection of data and individual privacy is also instrumental to many other rights, such as personal liberty, dignity, equality, fairness, and justice. Furthermore, in the long term, insufficiently observing privacy and data protection may erode (minimum levels of) trust between employers and employees. Such trust is necessary for employees to focus on their work (rather than on their safety and their position), which is in turn beneficial for employers.