


*Paweł Nowik** <https://orcid.org/0000-0002-1824-0884>

BIG DATA ANALYTICS IN THE ALGORITHMIC MANAGEMENT PROCESS: THE CASE OF TRANSPORT PLATFORMS IN THE GIG ECONOMY

Abstract. Gig economy business models are based on the mass automation of management decisions and workplace surveillance, which require using vast amounts of data and conditioning the algorithmic management system to function optimally. As a result, data has become an increasingly valuable and strategic economic resource. Ride-hailing platforms were a pioneer in this area. The privacy policies of transport platforms such as Bolt, Uber, and Deliveroo specify the use of data to train machine learning algorithms, which form the basis of automated decision-making. The accumulation of data and the asymmetry of information on these platforms leads to a serious violation of privacy rights. As companies collect more and more data about us, we lose control over how that data is used. This issue was highlighted a few years ago by Professor Shoshana Zuboff, who used the term “surveillance capitalism”. Within its framework, the human rights category of the right to privacy becomes the new free raw material for producing behavioural data, and the current article aims to analyse this phenomenon.

Keywords: Big data, algorithmic management, surveillance capitalism, transport platforms, machine learning

BIG DATA ANALYTICS W ZARZĄDZANIU ALGORYTMICZNYM: STUDIUM PRZYPADKU PLATFORM TRANSPORTOWYCH W EKONOMII WSPÓLDZIELENIA

Streszczenie. W artykule omówiono wpływ modeli biznesowych ekonomii gig na prywatność, szczególnie w kontekście platform transportowych, takich jak Bolt, Uber czy Deliveroo. Centralnym elementem jest zarządzanie algorytmiczne, które polega na automatyzacji decyzji i nadzorze miejsc pracy przy użyciu ogromnych ilości danych do szkolenia algorytmów uczących się maszynowo. Podkreślono, że dane stały się strategicznym zasobem ekonomicznym, prowadzącym do naruszeń praw do prywatności z uwagi na akumulację danych i asymetrię informacji. Profesor Shoshana Zuboff nazwała to zjawisko „kapitalizmem nadzoru”, gdzie prywatność staje się surowcem do produkcji danych behawioralnych. Artykuł zwraca uwagę na potrzebę znalezienia równowagi między wykorzystaniem danych przez sztuczną inteligencję a ochroną praw do prywatności, podkreślając znaczenie przejrzystości w praktykach zbierania i przetwarzania danych. Autor

* The John Paul II Catholic University of Lublin, pawelnowik@kul.lublin.pl

proponuje czteroetapowy proces zapewniający ochronę prywatności pracowników na platformach transportowych, zgodnie z międzynarodowymi standardami. Zostaje również poruszona kwestia wpływu systemów decyzyjnych opartych na AI na autonomię i prywatność pracowników, wzywając do opracowania optymalnych mechanizmów prawnych do oceny danych behawioralnych.

Słowa kluczowe: Big data, zarządzanie algorytmiczne, kapitalizm nadzoru, platformy transportowe, uczenie maszynowe

1. INTRODUCTION

Algorithmic management is a fundamental mechanism for decision-making across different platforms of work within the gig economy. It involves the use of various technological tools and techniques to remotely manage workers and facilitate automated or semi-automated decision-making processes. This type of management relies on algorithms and data collection to monitor and supervise workers, assign tasks, determine pay rates, and evaluate performance (Mateescu, Nguyen 2019, 1–3).

A prerequisite for effective algorithmic management is access to a wide range of reliable data (Gillespie 2014, 167–193). In contrast to traditionally perceived management models based on personal relationships – algorithmic relationships – algorithmic management depends on the continuous transfer of information about the behaviour of individual employees (Rosenblat, Stark 2016, 3758–3784). Ride-hailing platforms such as Uber and Lyft utilise algorithmic management to optimise matchmaking, pricing, and driver performance assessment. However, using these algorithms raises concerns about potential biases and the lack of human oversight in decision-making processes. Additionally, collecting and processing vast amounts of data on riders and drivers raises ethical considerations concerning privacy, data security, and potential misuse of personal information. The potential creation of detailed profiles and data-sharing without user consent further exacerbates these concerns. Therefore, it is imperative to ensure transparency in data collection and processing practices to safeguard the privacy and rights of riders and drivers.

Despite these concerns, the research in this area is still insufficient. The main research challenge presented in this article concerns the delicate balance between the data used by artificial intelligence in the digital economy and the protection of individuals' right to privacy. The text highlights the concentration of data among several companies as well as individuals' lack of access and control over their data. Analytical techniques – such as data exploration and predictive analytics in the employment sector – also raise new concerns about privacy and data protection. The article elaborates on the concept of privacy as a fundamental human right and underlines the need to establish clear legal standards and safeguards against unwarranted intrusions into the privacy of individuals, whether

by public authorities or private entities. It aptly points out that a holistic approach is crucial, encompassing the ethical complexities associated with technological advances and the imperative to safeguard the right to privacy in an ever-expanding data-driven economy.

The first part of this article looks at the problematic use of data in algorithmic management systems within gig economy business models. These models rely heavily on extensive management decisions and the automation of workplace monitoring, requiring large amounts of data to condition the entire algorithmic management system. Unfortunately, many platforms tend to regard the data they collect as their own, even though it is generated by users. In some cases, platforms explicitly list data as an asset in their annual reports. This issue has been highlighted by Professor Shoshana Zuboff in her book titled *The Age of Surveillance Capitalism*, in which she critiques the peculiar “new economic order” that treats human experience (behavioural data) as free raw material for hidden commercial practices of extraction, programming, and selling (Zuboff 2019).

The text also explores the various sources of data used for algorithmic management practices and the process of preparing that data for use. Data can come from a variety of sources, including APIs, databases, and files, but it often needs to be cleaned, structured, and standardised before it can be used.

The research question of the second part of the article revolves around the recognition of the right to privacy and data protection as fundamental human rights, as recognised by international and regional instruments. In particular, the text emphasises the need for companies to uphold these rights and highlights the importance of conducting human rights due diligence (HRDD) as well as implementing workplace privacy policies to protect the privacy rights of their employees, especially those working on transport platforms. To address this issue effectively, the author proposes a four-step process. This includes mapping the privacy footprint, conducting a privacy gap analysis, prioritising actions and mitigations, and embedding privacy in the workplace.

The aim is to enable companies to implement robust privacy policies while respecting the rights of their employees and complying with international and regional standards. By following this proposed approach, companies can take proactive steps to protect the privacy of their employees’ data in the context of the gig economy and the specific challenges faced by workers in the transport sector.

The third part of the article focuses on issues related to the right to privacy in the light of algorithmic governance. In particular, the text discusses the interpretability and applicability of several European solutions proposed by the EU and the Council of Europe.

Implementing algorithm-based decision-making systems in the workplace raises concerns about privacy and human autonomy, which are fundamental human rights. Research indicates that when AI systems make decisions that have serious employment consequences, employees can often feel helpless and

alienated, experiencing a lack of respect for privacy and increased scrutiny. The author highlights three main areas of concern: the collection and use of employee data, the protection of privacy in the workplace, and the lack of appropriate and transparent AI-based decision-making systems. The author suggests that optimal legal mechanisms should be developed to assess the appropriate classification of behavioural data, as the effectiveness and efficiency of ADM systems both depend on the acquisition of large amounts of data.

2. DATA – AN ESSENTIAL RESOURCE

Gig economy business models rely heavily on the automation of critical management decisions and workplace surveillance, which requires the use of vast amounts of data to condition the functioning of algorithmic management systems. Ride-hailing platforms have been at the forefront of pioneering these practices (Lee et al. 2015, 1603–1612). In its broadest sense, an algorithm refers to a process or set of rules followed in computation or other problem-solving operations, especially by a computer (Nowik 2021, 2). Therefore, an algorithm is essentially a computational formula that autonomously makes decisions based on statistical models or decision rules without the need for direct human intervention (Duggan et al. 2020, 114–132). In this context, algorithmic management can be understood as a diverse set of technologies used to remotely manage employees, including data collection and employee monitoring to enable automated or semi-automated decision-making (Mateescu, Nguyen 2019; Walker, Fleming, Berti 2021, 26–43; Montaudon-Tomas, Pinto-Lóp, Amsler 2022). Indeed, data has become an increasingly valuable and strategic economic resource (Rani, Singh 2019). Unfortunately, platforms often consider the data they collect as their property, even though it is generated by users (employees, customers, and clients). Some platforms explicitly list data as an asset in their annual reports (Baiocco et al. 2022, 12).

This problem was highlighted a few years ago by Professor Shochana Zuboff in her celebrated monograph titled *The Age of Surveillance Capitalism*. In this Harvard study, the author undertook a frontal critique of the peculiar “new economic order” that considers human experience (behavioural data) as the free raw material of the hidden commercial practices of extraction, programming, and sales. Professor Zuboff uses the term “surveillance capitalism”, wherein the human rights category of the right to privacy becomes the new free raw material for producing behavioural data. Some of this data is used to improve products and services, while the rest constitutes the so-called “surplus data” (behavioural surplus), which is used in advanced production processes referred to as “machine intelligence.” The behavioural surplus becomes a product of predictive analytics, which aims to implement processes for predicting current, future, and horizontal

behaviour. Furthermore, these predictive products are traded in new markets for behavioural predictions, which, among other things, can improve other technologies that apply algorithmic management (Zuboff 2019, 94)

The privacy policies of various platforms explicitly mention the use of data for training machine learning algorithms and automated decision-making processes. For example, Uber explicitly mentions the use of data for automated decision-making, facilitating dynamic pricing, matching drivers and passengers, and deactivating users with low ratings (Baiocco et al. 2022, 12; Cram et al. 2022, 426). Similarly, online platforms Freelancer and Upwork specify that they use data for automated decision-making in tasks such as matching freelancers with clients and improving machine learning algorithms (Baiocco et al. 2022, 12).

This data-driven approach helps to improve the overall efficiency and effectiveness of their services. The collected data allows platforms to develop an efficient matching system and gives them new control over workers (Baiocco et al. 2022, 12). In addition, data and information asymmetries on these platforms create power imbalances in exercising management control, including the monitoring of driver behaviour, the simulation of ETA (Estimated Time of Arrival), customer ratings, job acceptance and completion rates, interaction with support staff, availability, surveillance for ensuring driver safety and identification, the use of fraud detection and facial recognition technology, driver profiles that include “fraud probability scores” in the automated job allocation decision-making process, and automated fare setting (Cansu, Farrar 2021, 13). Platforms often exercise this control through their design features and algorithms programmed by humans to transform data into the desired output (Baiocco et al. 2022, 12). These practices reflect the platforms’ use of data to exert control and influence various aspects of their operations. The implementation of sophisticated technologies, such as facial recognition and fraud detection, adds to the complexities of the management processes on these platforms. The cited study by the International Labour Organisation (ILO) in 2022 sheds light on the significance of these data-driven mechanisms in shaping the dynamics between platform operators and their drivers. Such insights contribute to our understanding of the broader implications of technology adoption in the gig economy (Baiocco et al. 2022).

3. THE RIGHT TO PRIVACY AS A CATEGORY OF HUMAN RIGHTS

The concentration of data among a few organisations in the digital economy is a threat not only to privacy but also to users’ rights. Data should be treated as a right of those who generate it, not as an asset belonging to the company or platform that collects it (Baiocco et al. 2022, 12). In most jurisdictions, except for the EU, employees have no access to or control over their data and have very little information about its use. The availability of data on a massive and unprecedented

scale, combined with increased computing power and cloud infrastructure for data storage, has led to significant breakthroughs in AI technologies (Baiocco et al. 2022, 12). The global standards and common elements of data protection emerge from existing studies, which have compared and synthesised the main data protection standards. The leading study in this area was conducted in 2020 by the Global Privacy Assembly (CAIDP 2021, 30).

The challenges of people analytics raise privacy concerns. Techniques such as data mining as well as predictive and contextual analytics highlight critical privacy and data protection issues in the workplace (FRA 2010, 12). The essence of the right to privacy, as traditionally understood, is the prohibition of interference by others in a person's personal life unless, under certain circumstances and conditions, the law allows that the right to privacy in the context of algorithmic management is at risk throughout the data lifecycle. In the context of transport platforms, privacy concerns relate primarily to the data collection phase (behavioural data), which raises the issue of the autonomy of employees to exercise adequate control over their privacy. One source of this privacy issue is knowledge asymmetries, wherein the analysis may contain errors that result in discrimination against a group of employees or individual employees (Hong 2016). Furthermore, when deleting data, the platform may underestimate the importance of "forgetting" employee data. Behind algorithmic management lies a conflict between the need to process data, which is the modern "fuel" of technological development, and the need to protect the right to privacy (Rahul, Shruti Aji 2020, 64). On the one hand, companies, including platforms, promote the need to develop ethical AI and algorithmic management. On the other hand, a high priority of HR departments is developing Business Intelligence technology by collecting and processing as much data as possible. This dilemma illustrates the path to be followed when seeking solutions in this area (Koops, Leenes 2014, 159). As such, an integrated approach, considering both the ethical challenges of developing new technologies and a multidisciplinary and global approach, is required to safeguard the right to privacy in the data-driven economy.

The concept of "privacy" is interdisciplinary and not only of interest to the legal sciences. Article 13 of the Universal Declaration of Human Rights adopted by the United Nations (UN) prohibits arbitrary interference with one's private life, family, home, and correspondence. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) derives from state parties' obligation to refrain from arbitrary and unlawful interference with private life. Furthermore, the state must create legal norms for protection against such interference by both public authorities and private actors. The state party is thus obliged to take appropriate legislative measures to prevent unacceptable interference with an individual's right to privacy and, simultaneously, to ensure that this right can be exercised effectively by the individual.

Much about what the standard of protection for the right to privacy should look like is stated in a decision of the Human Rights Committee (Coeriel et al. vs. The Netherlands, Communication No. 453/1991 (1994)). It was stated that “the concept of privacy refers to that sphere of a person’s life in which he or she can freely express his or her identity, both by entering into relationships with others and on his or her own.” Furthermore, General Comment No. 16 to Article 17 points out that the collection and storage of personal data in computers, data banks, and other devices, whether by public authorities or by private individuals or entities, must be regulated by law (Vega Gutiérrez 2017, 444). Therefore, states must take adequate measures to ensure that information concerning a person’s private life does not end up with persons who are not authorised by law to receive, process, and use it, and that it is never used for purposes contrary to the Covenant (Della Fina, Cera, Palmisano 2017, 327–337; Vega Gutiérrez 2017, 445). For the most effective protection of one’s private life, everyone should have the right to determine in an intelligible form whether – and if so, what – personal data are stored in automated databases and for what purposes. Each person should also be able to determine which public authorities, private persons, or entities control or may control his/her data files. Furthermore, if such files contain inaccurate personal data or have been compromised or processed in breach of the law, every person should have the right to request their rectification or erasure’ (CCPR General Comment No. 16: Article 17 (Right to Privacy) 1988).

The challenges of people analytics raise privacy concerns. Techniques such as data mining, predictive and contextual analytics highlight critical privacy and data protection issues in the workplace (Hendrickx 2022, 18). The regional or global standards were analysed, including – in addition to the Assembly’s own “Madrid Resolution” – the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the Council of Europe (CoE) Convention 108, the Standards for Personal Data Protection for Ibero-American States, the African Union Convention on Cyber Security and Personal Data Protection, the Economic Community of West African States (ECOWAS) Data Protection Act, the EU GDPR, and the UN Guidelines for the Regulation of Computerised Personal Data Files. The Global Principles from Comparisons (Hendrickx 2022, 11ff; GPA 2020, 7) are as follows:

- Fairness: Treat data fairly (non-discrimination, transparency, no fraud).
- Legality: Processing lawfully for legitimate purposes.
- Purpose specification: Specific, lawful processing.
- Proportionality: Consideration of data minimisation, adequacy and inappropriate processing.
 - Data quality: Ensure accuracy, completeness and timeliness.
 - Openness: Transparent policies, availability of information.
 - Security: Secure processing of personal data.

- Data Retention: Limiting data retention to processing needs.
- Accountability: Hold data controllers accountable.
- Access: Access, rectification, erasure, objection (in some cases) by data subjects (GPA 2020, 7).

In addition, both Article 12 of the Personal Data Protection Commission (PDPC) Singapore and Article 17 of the ICCPR, as well as several other international and regional instruments, recognise the right to data privacy as a fundamental human right.

A significant strength of the human rights approach is that the right to privacy and data protection is the focal point of attention (Ebert, Wildhaber, Adams-Prassl 2021, 1). The UN framework unequivocally recognises that under international human rights law, states must protect everyone within their territory and/or jurisdiction from human rights violations. This obligation suggests that states must have adequate laws and regulations to prevent and address human rights violations in business and ensure access to an effective remedy for those whose rights have been violated (UN Working Group 2023). In addition, the UN framework addresses the human rights obligations of businesses. Businesses must respect human rights, regardless of the size, industry, or location of operation. Such accountability indicates that companies must be aware of their actual or potential impact, prevent and reduce abuse, and address the negative impacts caused by them in all areas of their operations. In June 2011, the UN Human Rights Council established a “working group on human rights issues and transnational corporations and other business enterprises”, commonly referred to as the Working Group on Business and Human Rights, composed of five independent experts for a duration of three years (Office of the United Nations High Commissioner for Human Rights 2022). The mandate of the working group was renewed in 2014, 2017, and 2020. In addition, the UN Guiding Principles on Business and Human Rights (UNGPs) were unanimously endorsed by the UN Human Rights Council in 2011 (Office of the United Nations High Commissioner for Human Rights 2022). According to the UNGPs, all companies have a corporate responsibility to respect human rights throughout their business operations, and a process of continuous human rights due diligence (HRDD) is an essential requirement for companies in fulfilling this responsibility (B-Tech Project OHCHR and Business and Human Rights n.d.). Due diligence, according to Business and Human Rights (B&HR), is not only a legal or technical process but also a multidisciplinary managerial stance to uphold ethical values by respecting human rights throughout a company’s operations and integrating the voices of rights holders (Ebert, Wildhaber, Adams-Prassl 2021, 2; Monnheimer 2021, 9–46). Guided by the B&HR rationale, companies should conduct due diligence on the human rights impacts of their operations, including on employee privacy. Private employers should, therefore, respect the right of their employees to privacy as a category of human rights.

The UNGPs set out the legal and policy implications of implementing this obligation through a “smart mix” of measures, including legally-binding measures, mainly where voluntary measures still leave significant gaps in human rights protection (B-Tech Project OHCHR and Business and Human Rights n.d.) Based on the human rights category, this regulatory approach is designed to create a wave of legal requirements for responsible businesses affecting global markets. Based on the requirements of the UNGPs, companies must formulate workplace privacy policies and implement them using a due diligence process (Ebert, Wildhaber, Adams-Prassl 2021, 7). Businesses must respect human rights, with privacy as a gateway to propose tailored privacy due diligence. The UNGPs lack specific human rights template; operationalised differently. They focus on rights holders and harm reduction in due diligence (Ebert, Wildhaber, Adams-Prassl 2021, 8). The privacy due diligence model proposed in the current study is based on a four-step process: (1) mapping the privacy footprint; (2) privacy gap analysis; (3) the prioritisation of measures, mitigation, and management; and (4) anchoring privacy in the workplace (Ebert, Wildhaber, Adams-Prassl 2021, 8).

It is, therefore, worth examining this method in the context of protecting the data privacy of those employed by transport platforms. Privacy footprint mapping is a valuable method for protecting the privacy of transport platform employees. This process involves engaging a wide range of stakeholders to understand the privacy implications of a company’s workforce monitoring practices. In the case of transport platforms, the circle of interested groups is wide. Stakeholders may be employees of the company and rights holders negatively affected by the breach of employee privacy, such as their partners or children. Strategic stakeholder engagement is at the heart of B&HR’s due diligence. It differs from traditional consultation in that it is based on the rights holder’s perspective. Rapid technological advances mean that some stakeholders may not be able to understand or predict the negative consequences of a data breach. They may not be aware of the technological and analytical capabilities of what is being measured or what conclusions can be drawn (functional sprawl). Privacy due diligence can address the imbalance of bargaining power between employees and employers, as it may go beyond the terms of the employment contract (Ebert, Wildhaber, Adams-Prassl 2021, 8). Organisations need to identify and assess the privacy implications of their actions. This includes identifying the groups of employees most affected by privacy issues and understanding how these groups may be vulnerable. A Privacy Impact Assessment (PIA) is a valuable tool for this purpose. A PIA should be conducted as part of privacy due diligence and should involve a hybrid model of internal and external stakeholder engagement (Ebert, Wildhaber, Adams-Prassl 2021, 8).

The second step is a privacy gap assessment. This involves identifying the existing processes and potential privacy gaps. The assessment goes beyond the legal framework to address issues arising from regulatory gaps or changing

legal concepts in different jurisdictions. This helps to create a robust corporate privacy policy across jurisdictions. Privacy due diligence can identify and address emerging privacy gaps more effectively than a purely legal or technical assessment (Ebert, Wildhaber, Adams-Prassl 2021). Although most decisions are made internally, the decision-making process should be subject to broader stakeholder engagement practices and human rights requirements. Therefore, the gap assessment consists of at least two steps: first, meeting the necessary legal requirements, such as considering context, proportionality, consent, and establishing a clear interpretation of legal terms and technological safeguards; and, second, considering the ethical challenges to privacy (legal grey areas) that may lead managers or employees into a socio-technical dilemma (Ebert, Wildhaber, Adams-Prassl 2021, 9).

The third step is privacy impact mitigation. This involves identifying the most serious privacy risks and prioritising their mitigation. The organisation must then determine how to address the privacy gaps identified in the second step. For example, due diligence may reveal that data-driven monitoring is not the best solution for balancing productivity and privacy. In contrast, a geo-location tracking system that follows a van to send notifications to customers when a package arrives may seem less controversial at first glance. However, it could become controversial if the truck's movements are used to dictate when an employee can go to the bathroom or take a lunch break (Ebert, Wildhaber, Adams-Prassl 2021, 10).

The final step is to embed privacy due diligence into business practice. This involves ongoing reporting, assessing, and learning about the privacy impacts of the company's activities. For example, the company should assess whether specific accountability and oversight mechanisms are in place to monitor the workplace. The company should also consult with stakeholders to ensure that these mechanisms are effective. The UNGPs suggest that operational grievance mechanisms should be directly accessible to stakeholders who may be adversely affected. Integrating privacy due diligence into business practices should also include preventive and remedial mechanisms to address negative privacy impacts (Ebert, Wildhaber, Adams-Prassl 2021, 10).

Privacy due diligence can only complement litigation. The model requires an understanding of how organisations can use technology without violating privacy as well as how stakeholders understand the technology and their options for action. Human rights-based methodologies have been criticised for failing to promote the collective voice of workers. One strategy is to ensure that the collective and individual voices of workers are heard through ongoing engagement with stakeholders such as trade unions, works councils, or other worker representative bodies. The right to privacy is linked to other fundamental rights, such as freedom of association and expression (Ebert, Wildhaber, Adams-Prassl 2021, 10).

4. THE BRUSSELS AND STRASBOURG EFFECTS – THE MULTIPLICATION OF EUROPEAN MODELS

Another method of regulating privacy rights issues in the light of algorithmic governance is to interpret and apply multiple solutions proposed by the EU and the Council of Europe (Bygrave 2020, 1).

Under EU regulations, privacy and data protection are overlapping and strongly interdependent legal concepts. Central to the European human rights protection system is the European Convention on Human Rights (ECHR), drawn up in Rome on 4th November, 1950, and ratified with prior consent by law. Article 8 of the ECHR indicates that “Everyone has the right to respect for his private and family life, his home, and his correspondence” (para. 1). “No interference by a public authority with the exercise of this right shall be permitted except in cases provided for by law and necessary in a democratic society for reasons of national security, public safety, or the economic well-being of the country, the protection of law and order and the prevention of crime, the protection of health and morals, or the protection of the rights and freedoms of others” (para. 2). The right to privacy described in Article 8 of the ECHR primarily protects the individual against arbitrary interference by public authorities. However, as emphasised in the European Court of Human Rights case law, the duty to refrain from such interference does not exhaust the obligations incumbent on state parties to the ECHR. In addition to the negative obligations, there are certain positive obligations to ensure adequate respect for private life. This includes adopting appropriate measures to ensure respect for private life and relations with private persons. Respect for private life also extends to privacy in the workplace, as recognised by the European Court of Human Rights in *Niemietz vs. Germany* (1992). The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) opened for signature on 28th January, 1981, and was the only legally-binding international instrument in the field of data protection until 2018. The notion of ‘personal data’, which the Convention aims to protect, is understood to mean any information relating to an identified or identifiable natural person (Article 2(a) of the Convention). It is, therefore, not surprising that both in the Preamble and in Article 1, the Convention emphasises the vital link between the protection of personal data and the right to privacy. As emphasised in the Preamble of the Convention, one of the primary motives for adopting this legal instrument was to reconcile the need to protect human rights and fundamental freedoms, including the right to privacy, with the freedom of information to flow regardless of frontiers.

Privacy issues are primarily addressed by Articles 7 and 8 of the Charter of Fundamental Rights (CFR) of the European Union, declared on 7th December, 2000, which, according to Article 6(1) of the Treaty on the Functioning of the

European Union (TFEU), has the same legal value as a treaty. However, in the light of Article 51 of the CFR, its provisions apply to the institutions, bodies, offices, and agencies of the Union and the Member States to the extent that they apply Union law. That being said, it cannot be considered that the CFR does not affect civil law. According to Article 7 of the CFR, “Everyone has the right to respect for private and family life, home, and communications”. As is the case of other human rights instruments, the Charter links the issue of privacy with the issue of human dignity, which – as underlined in the Praesidium of the Convention that drafted the Charter – is not only a fundamental right in itself but also constitutes the objective basis of fundamental rights. Consequently, the right to privacy cannot be used to attack another person’s dignity. In the European Union law, privacy is also implemented through data protection provisions. Prior to the Treaty of Lisbon, the treaties establishing the European Communities (EC) and the Maastricht Treaty (formally known as the Treaty on European Union) did not contain specific provisions on the protection of personal data. Today, Article 16(2) of the TFEU empowers the European Parliament and the Council to determine, following ordinary legislative procedure, the rules relating to the protection of individuals regarding the processing of personal data by the Union’s institutions, bodies, offices, and agencies, and by the Member States when conducting activities within the scope of the Union law, and the rules relating to the free movement of such data. One of the most robust privacy protection measures can be found in Article 22(1) of the GDPR, which grants employees “the right not to be subject to a decision based solely on automated processing... which produces legal effects concerning [them] or significantly affects [them] in a similar manner.” “Processing” refers to an operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction (Article 4(2) of the GDPR). By contrast, “profiling” refers to any form of automated processing of personal data that involves the use of personal data to evaluate personal factors relating to an individual, in particular to analyse or predict aspects relating to that individual’s performance, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements (Article 4(4), GDPR). The above prohibition does not apply if such a decision: a) is necessary for the conclusion or performance of a contract between the data subject and the controller; b) is authorised by the Union law or the law of a Member State to which the controller is subject and which provides for suitable measures to protect the rights, freedoms, and legitimate interests of the data subject; or c) is based on the data subject’s explicit consent (Article 22(2), GDPR). In the cases referred to in Article 22(2)(a) and (c) of the GDPR, the controller is obliged to implement appropriate measures to protect the rights, freedoms, and

legitimate interests of the data subject. Furthermore, the minimum intervention in case of an action contrary to the prohibition established in Article 22(1) of the GDPR creates an obligation for the controller to ensure that the affected person has the right to obtain the necessary assistance in the form of human intervention, not an automaton, consisting of the possibility for the affected person to express his/her position and to possibly challenge the unlawful decision (Article 22(3), GDPR). The decisions referred to in Article 22(2) cannot be based on special categories of personal data referred to in Article 9(1) unless Article 9(2)(a) or (g) applies and there are appropriate safeguards to protect the rights, freedoms, and legitimate interests of the data subject (Article 22(4), GDPR). As such, the processing of personal data to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic and biometric data to uniquely identify a natural person or data concerning a person's health, sexuality, or sexual orientation became prohibited (Article 9(1), GDPR). However, Article 9(1) does not apply if one of the following conditions applies: (1) the processing is necessary for reasons of substantial public interest, based on the Union law or a Member State law, which are proportionate to the aim pursued, do not undermine the essence of the right to data protection, and provide for suitable and specific measures to protect the fundamental rights and interests of the data subject; (2) the data subject has given his/her explicit consent to the processing of those personal data for one or more specific purposes.

It should be noted that the “right to explanation” does not receive mention in Article 22 of the GDPR, with the exception of recital 71, which leads to the broad issue of the interpretation of the GDPR in European legislation regarding the legal status of recitals. In the context of the right to explanation, the wording “should” in the recital further weakens the institution. Article 22 also provides the right not to be subjected to a decision based solely on “automated processing, including profiling, which produces legal effects against it (...)” This important threshold practically excludes algorithmic management, which entails full automation of decisions in EU countries and which has no significant human input in such decisions. In addition, several principles of the GDPR apply to general data collection and processing technologies. These include, in particular, the right to transparent information and communication, the right to access Articles 12, 13, and 15, as well as the rectification, erasure, and restriction of processing Articles 16 and 17. Article 22 is, therefore, an unstable legal basis for building a harmonised, general EU right to algorithmic clarification. Moreover, Article 22 contains an additional ambiguity – to operationalise the right to explanation, it is necessary to know the relevant input variables of the data (see steps one to four), which in itself requires access to part of what resembles an algorithmic explanation.

Stakeholders, EU authorities, and legal experts agree that it is challenging to successfully implement AI without causing disproportionate negative impacts

on workers. In their view, the data collection and processing capabilities of digital technologies require strong safeguards to preserve workers' data protection and privacy rights as well as the possibility of redress, and to enable better enforcement of the existing laws (Madinier 2022, 3).

The European Parliament's Special and Temporary Committee on Artificial Intelligence in a Digital Age (AIDA) called in its final report in April 2022 for the EU to take action and promptly put in place a favourable framework for AI capable of ensuring effective governance, sustainable and ethical standards, and freedom for innovation while avoiding over-regulation (AIDA 2022).

Among the main initiatives at the EU level to regulate AI are the European Commission's proposal for an AI Act and a Directive on improving working conditions in platform work. Both proposals address the issue of the regulation of algorithms in the workplace.

A draft of the artificial intelligence regulation presented by the European Commission in April 2021 sets out a regulatory structure that prohibits specific AI applications that are considered to have unacceptable risks, imposes compliance requirements on high-risk applications (e.g. mandatory human oversight and proof of security), and lightly regulates low-risk AI systems. The proposed AI regulation classifies AI systems "used in employment, employee management, and access to self-employment, in particular for recruitment and selection of individuals, decisions on promotions and terminations, and assignment of tasks, monitoring or evaluation of individuals at work." Furthermore, the regulation regards contractual relationships as high-risk. This indicates that such AI systems are subject to requirements, such as *ex-ante* compliance assessments concerning risk management, transparency, oversight, and cyber security, before being introduced and used in the EU single market.

On 9th December, the European Commission proposed a directive to improve working conditions for platform workers. The directive aims to define the employment status of platform workers and give them access to labour and social rights. However, few EU Member States have adopted national legislation to improve working conditions or provide social protection for platform workers. National legislation often only indirectly addresses the challenges of platform work and focuses on specific sectors, such as ride-hailing and delivery services. To date, there have been more than 100 court rulings and 15 administrative decisions in the EU on the employment status of platform workers. In most cases, judges have ruled that independent contractors should be reclassified as employees and platforms as employers.

The directive also aims to improve transparency, rights, and accountability in algorithmic management on digital labour platforms. This will help workers understand how tasks are allocated and prices set, and allow them to challenge decisions that affect their working conditions. The directive also aims to improve the enforcement and traceability of work on platforms, including in cross-border

situations. Platforms will be required to declare work in the country where it is carried out and to make information about their workers and working conditions available to national authorities. The Directive introduces the need for platform workers and their representatives to be informed and consulted on decisions relating to the management of algorithms. Platforms will also be required to facilitate channels of communication between workers and their representatives. The draft directive empowers self-employed workers, including those working for digital labour platforms, to influence and improve working conditions through collective bargaining and enhanced social dialogue (European Commission 2021).

The Directive uses the term “algorithmic management” to refer to IT-driven automated monitoring and decision-making systems that are increasingly replacing the functions of managers in companies, such as assigning tasks, monitoring and evaluating work performed, providing incentives, or imposing sanctions. Digital work platforms use algorithmic systems to organise and manage the people working for them through their applications or websites. Many platform workers often lack information about how algorithms work and how decisions are made. This includes a lack of information about how personal data is used. According to the Directive, individuals working for digital labour platforms will have the right to receive information about the automated monitoring and used decision-making systems and how they affect their working conditions. For example, they will receive information on how they are monitored, supervised, and evaluated, including by clients. They will also receive information on the automated systems that lead to or support relevant decisions, such as assigning tasks, proposing fees, and awarding bonuses. Employee representatives and labour authorities will also have access to such information (European Commission 2021).

Undoubtedly, the algorithmic management of employees should be fair and transparent. Any disclosure of automated decision-making should always include an explanation of the impact of these systems on employees. Article 6(2)(B) of the Directive states that the main parameters taken into account by automated decision-making and monitoring systems should be disclosed to platform employees, but no further guidance is provided, which leaves platforms with considerable room for abuse of their discretion. Without a further definition of the level and scope of information that the platform should provide, there is a high risk that employers will provide only cursory information that is decontextualised and of little practical use. Article 6(2) should be revised to include a clear call for disclosure of information regarding the factors for assessing employee performance, any form of profiling, the basis for decisions to reward or motivate employees, and the expected impact of automated decision-making in these areas. In addition, Article 6(3) should be modified to include an obligation for platforms to clarify, following the Common Standard, the purpose of algorithmic decision-making systems in terms of rationale, accountability, the use of personal data (including profiling), fairness, security and efficiency, and impact. Moreover,

Article 6(5) should be amended to prohibit using biometric authentication systems on platform workers. Collecting and processing biometric data to authenticate the identity of platform workers is unnecessary and disproportionate. In addition, the inaccuracy of facial recognition technologies, such as the Microsoft Azure Face API used by Uber, has been widely demonstrated, mainly when used on people of colour and other minority groups (Worker Info Exchange 2021). However, even when these systems work as intended, they pose unnecessary risks by collecting, processing, and often storing sensitive employee biometric data. Other identity authentication methods are less intrusive, equally or more reliable, and do not involve the same set of risks as biometric authentication. An additional threat to fundamental human rights is the existing practice of some platforms to share data with police and security services on demand without a warrant. For example, Uber operates a law enforcement and public health portal through which police and public authorities can request data. When Uber was denied a licence by the Transport for London in 2020, the UK's National Police Chiefs' Council lobbied the Transport for London Commissioner, because Uber had become a strategic source of intelligence (Worker Info Exchange 2021).

Many platform employers track employee behaviour and perform predictive analytics to create a “probability of deception scores” (Worker Info Exchange 2021), which are then used in automated work allocation and other performance management decisions. Using such technologies raises serious ethical concerns and poses unacceptable risks to fundamental human rights, including labour rights. Furthermore, the standardisation of such behavioural tracking and prediction could lead to further interference and abuse. For example, platforms could use predictive profiling of employee behaviour to draw unfair conclusions, including the likelihood that an employee will engage in union activity or enter into a legal dispute with the platform's employer. Accordingly, Article 6(5) should be amended to prohibit the use of employee behaviour profiling that: (1) categorises employees according to sensitive, protected characteristics or attributes; (2) makes predictions about employee behaviour; and (3) is used for or contributes to work allocation and performance management decisions.

The Directive prohibits digital work platforms from collecting or processing personal data that is not directly related to the work performed. Platforms must also refrain from collecting data when a person is not logged into the relevant app or website. Platforms must monitor and assess the impact of individual decisions made or supported by automated monitoring and decision-making systems on working conditions, such as pay or working hours. Workers have the right to receive an explanation of, and to challenge, significant automated decisions that affect their working conditions. Platforms must ensure that workers have access to human contact to discuss decisions that significantly affect them. Platforms must respond to requests to review decisions within one week. If a decision violates

a worker's rights, the platform must correct its actions or provide compensation (European Commission 2021).

Employees should have the right to complete access to and the portability of their data directly to any data controller designated by them, including regulators and employee representatives. Under the GDPR, data subjects have the right to access and port their data. However, while most platforms make some form of provision for employee access to their data, most omit the categories of data most relevant to the interrogation of fair pay, work allocation, safety, and security. As a rule, employees seeking access to comprehensive data must navigate complex automated request processes (dark patterns) as well as long and cumbersome administrative processes to obtain a response. To address this gap, Article 6(3) should explicitly mandate digital labour platforms to provide employees with comprehensive and meaningful access to input data (provided by the employees themselves), observed data (based on employees' use of the platforms, such as, for example, raw location measurements), and telematics data (inferred data based on observed data, such as the profiling of employee behaviour in the form of performance or risk and fraud assessments) (Cansu, Farrar 2021, 41). Platforms should provide such data in its entirety at the first request for access to data and should not attempt to use a differentiated or layered approach to providing access or data portability. Regulators and employee representatives should also have access to this data to investigate working conditions and possible direct or indirect cases of discrimination.

5. CONCLUSION

Using algorithmic decision-making systems in the workplace raises concerns about privacy and human autonomy, which are fundamental human rights. Research shows that employees can feel powerless and alienated when AI systems make decisions with significant employment consequences and a lack of privacy and scrutiny. However, few mechanisms have been developed to address privacy intrusions, as international law directly suggests. The main concerns include the collection and use of employee data, the protection of privacy in the workplace, and a lack of transparent and effective algorithmic decision-making systems.

In the context of atypical employment, such as digital labour platforms, the right to privacy can be threatened as algorithmic management relies on sharing employee behavioural data, such as private conversations and health status. However, the legal mechanisms for assessing the appropriate classification of behavioural data are inadequate.

The efficiency of algorithmic decision-making systems depends on acquiring vast amounts of data. Even if a state limits behavioural data acquisition, another source remains for global online platforms. The ride-hailing industry also raises

similar concerns about privacy and human autonomy. Drivers must share their location data, which can be misused. Further research is necessary to understand the implications of algorithmic decision-making systems on privacy, human autonomy, and employment rights as well as to develop mechanisms to address any negative impacts.

BIBLIOGRAPHY

- AIDA. 2022. *Special Committee on Artificial Intelligence in a Digital Age*.
- Baiocco, Sara. Enrique Fernandez-Macias. Uma Rani. Annarosa Pesole. 2022. *The Algorithmic Management of work and its implications in different contexts*. ILO.
- Bygrave, Lee A. 2020. "The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects." *Computer Law & Security Review* 40.
- CAIDP. 2021. *Artificial Intelligence and Democratic Values*. Washington, DC: Center for AI and Digital Policy.
- Cansu, Safak. James Farrar. 2021. *Managed by Bots. Data-Driven Exploitation in the Gig Economy*. Worker Info Exchange.
- Cram, W. Alec. Martin Wienerb. Monideepa Tarafdarc. Alexander Benlian. 2022. "Examining the Impact of Algorithmic Control on Uber Drivers' Technostress." *Journal of Management Information Systems* 39(2): 426–453.
- Duggan, James. Ultan Sherman, Ronan Carbery. Anthony McDonnell. 2020. "Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM." *Human Resource Management Journal*: 114–132.
- Ebert, Isabel. Isabelle Wildhaber. Jeremias Adams-Prassl. 2021. "Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection." *Big Data & Society* 8(1).
- European Commission. 2021. *Questions and answers: Improving working conditions in platform work*. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_21_6606/ (accessed: 25.07.2023).
- Fina, Valentina Della. Rachele Cera. Giuseppe Palmisano. 2017. *The United Nations Convention on the Rights of Persons with Disabilities. A Commentary*. Cham: Springer.
- FRA. 2010. "Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II." *Publications Office of the European Union*: 1–56.
- Gillespie, Tarleton. 2014. "The Relevance of Algorithms." In *Media Technologies: Essays on Communication, Materiality, and Society*. 167–193. Edited by Tarleton Gillespie, Pablo J. Boczkowski, Kirsten A. Foot. Cambridge: MIT Press Scholarship.
- GPA. 2020. "Policy Strategy Working Group 1: Global Frameworks and Standards."
- Hendrickx, Frank. 2022. "Protection of workers' personal data: General principles." *ILO Working paper* 62.
- Hong, Renyi. 2016. "Soft skills and hard numbers: Gender discourse in human resources." *Big Data & Society* 3(2).
- Koops, Bert-Jaap. Ronald Leenes. 2014. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law". *International Review of Law, Computers & Technology* 28(2): 159–171 .
- Lee, Min Kyung. Daniel Kusbit. Evan Metsky. Laura Dabbish. 2015. "Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers." In *CHI '15*:

- Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 1603–1612. New York, NY: Association for Computing Machinery.
- Madinier, Franca Salis. 2022. “A guide to Artificial Intelligence at the workplace.” European Economic and Social Committee.
- Mateescu, Alexandra. Aiha Nguyen. 2019. “Algorithmic Management in the Workplace.” *Data & Society*.
- Monnheimer, Maria. 2021. *Due Diligence Obligations in International Human Rights Law*. Cambridge: Cambridge University Press.
- Montaudon Tomas, Cynthia Maria. Ingrid N. Pinto-Lóp. Anna Amsler. 2022. “Discussions on How to Best Prepare Students on the Ethics of Human-Machine Interactions at Work.” In *Applied Ethics in a Digital World*. 216–237. Edited by Ingrid Vasiliu-Feltes, Jane Thomason. Hershey, PA: IGI Global.
- Nowik, Paweł. 2021. “Electronic personhood for artificial intelligence in the workplace.” *Computer Law & Security Review* 42.
- Rahul, Rai. Murali Shruti Aji. 2020. *Global standards on AI. A report on global legislation & policy positions governing AI technology*. INDI/ai.
- Rosenblat, Alex. Luke Stark. 2016. “Algorithmic Labor and Information Asymmetries: A Case Study of Uber’s Drivers.” *International Journal of Communication* 30(7): 3758–3784.
- UN Working Group. 2023. <https://www.business-humanrights.org/en/big-issues/un-working-group/> (accessed: 15.07.2023).
- Walker, Michael. Peter Fleming. Marco Berti. 2021. “You can’t pick up a phone and talk to someone: How algorithms function as biopower in the gig economy.” *Organization*, 26–43.
- Zuboff, Shoshana. 2019. *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*. Warszawa: Zysk i S-ka.