THE YALE LAW JOURNAL FORUM

JANUARY 31, 2025

Data Laws at Work

Veena Dubal

ABSTRACT. In recognition of the material, physical, and psychological harms arising from the growing use of automated monitoring and decision-making systems for labor control, jurisdictions around the world are considering new digital-rights protections for workers. Unsurprisingly, legislatures frequently turn to the European Union (EU) for inspiration. The EU, through the passage of the General Data Protection Regulation in 2016, the Artificial Intelligence Act in 2024, and the Platform Work Directive in 2024, has positioned itself as the leader in digital rights, and, in particular, in providing affirmative digital rights for workers whose labor is mediated by "a platform." However, little is known about the efficacy of these laws.

This Essay begins to fill this knowledge gap. Through close analyses of the laws and successful strategic litigation by platform workers under these laws, I argue that the current EU framework contains two significant shortcomings. First, the laws primarily position workers as liberal, autonomous subjects, and in doing so, they make a category error: workers, unlike consumers, are subordinated by law and doctrine to the firms for which they labor. As a result, the liberal rights that these laws privilege—such as transparency and consent—are insufficient to mitigate the material harms produced through automated labor management. Second, this Essay argues that by leaning primarily on transparency principles to detect, prevent, and stop violations of labor and employment law, EU data laws do not account for the ways in which workplace algorithmic management systems often create new harms that existing laws of work do not address. These harms, which fundamentally disrupt norms about worker pay, evaluation, and termination, arise from the relational logic of data-processing systems—that is, the way that these systems evaluate workers by dynamically comparing them to others, rather than by evaluating them objectively based on fulfillment of ascribed duties. Based on these analyses, I propose that future data laws should be modeled on older approaches to workplace regulation: rather than merely seeking to elucidate or assess problematic data processes, they should aim to restrict these processes. The normative north star of these laws should be proscribing the digital practices that cause the harms, rather than merely shining a light on their existence.

INTRODUCTION

Despite widespread legal concerns about the technology industry's surveillance of consumers,[1] the most intrusive and far-reaching digital technologies for monitoring and controlling human behavior do not target people when they make or contemplate purchases. They target people at work. In many jobs and sectors, particularly low-wage ones, digital workplace technologies execute novel forms of labor control. In some cases, they even replace human managers, whose social and technical knowledge about a job, the workplace, and a particular worker might otherwise be used to make hiring decisions, determine quotas, allocate work, decide pay, evaluate performance, and make disciplinary or termination decisions.[2]

A growing number of workers, including so-called "gig" and "platform" workers (broadly defined as workers who are completely managed through smartphone applications), are now hired, evaluated, paid, disciplined, and terminated through automated systems, with little to no meaningful human oversight or intervention.[3] Because platform companies often treat their workers as self-employed contractors who are not afforded the protection of established employment and labor laws, these firms have been uniquely positioned to experiment with remote algorithmic control and pioneer new forms of digitalized workforce management.[4] Platform work, in this sense, has been a canary in the coal mine. Innovative systems of automated worker control, which originated in the platform context, have since been imported to other employment sites—including in the transportation, delivery, warehousing, hospitality, janitorial, healthcare, computer-science, and education sectors.[5]

[1] For background on corporate surveillance of consumers and its potential social and political impacts, see SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); and JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019).

[2] See *infra* Section II.B.

[3] *Id.*

[4] For more on worker misclassification and platform companies, see Ruth Berins Collier, V.B. Dubal & Christopher Carter, *Labor Platforms and Gig Work: The Failure to Regulate* (Inst. for Rsch. on Lab. & Emp., Working Paper No. 106-17, 2017), https://escholarship.org/content/qt4c8862zj/qt4c8862zj_noSplash_62931d9a3c82dd7052d2faa3e55adb7b.pdf [https://perma.cc/25EL-ZF67].

[5] *See generally* Mohammad Hossein Jarrahi, Gemma Newlands, Min Kyung Lee, Christine T. Wolf, Eliscia Kinder & Will Sutherland, *Algorithmic Management in a Work Context*, 8 BIG DATA & SOC'Y (2021), https://doi.org/10.1177/20539517211020332 [https://perma.cc/P3HG-DYWM] (arguing that algorithmic management has spread from platform work to more standard employment to interface with existing organizational structures); ANTONIO ALOISI & VALERIO DE STEFANO, YOUR BOSS IS AN ALGORITHM: ARTIFICIAL INTELLIGENCE, PLATFORM WORK AND

These new systems of workforce management can be divided into two broad categories: automated monitoring systems (AMSs) and automated (and augmented) decision-making systems (ADSs).[6] AMSs collect a wide array of personal data from workers both on and off the job, including data on speed, movement, and behavior, and then feed that data into ADSs to carry out or support a broad range of tasks, such as determining work allocation, communicating with a worker (via a chatbot), or evaluating workplace performance. ADSs (or offline procedures that heavily rely on ADSs) are also sometimes used to perform the most central functions of the employer: to determine whether to hire a worker, how much to pay them, when to discipline or reward them, and critically, when to terminate them.[7]

Proponents of the digitalization of labor management—including artificial intelligence (AI) companies, data brokers, employers, and some scholars[8]—argue that digital labor-management systems bring machine objectivity into the workplace via digital on-the-job surveillance and control, thus bettering the lives of workers by purportedly increasing scheduling flexibility and correcting for longstanding gendered and racial wage differentials.[9] They also assert that these systems improve firm accuracy and efficiency while enhancing worker satisfaction.[10]

LABOUR (2022) (forecasting how digital tools used for management in platform will spread beyond it and arguing for regulation); Zephyr Teachout, *Algorithmic Personalized Wages*, 51 POL. & SOC'Y 436 (2023) (discussing how algorithmic wage setting has extended beyond ridehail work and typologizing various forms of it); JEREMIAS PRASSL, HUMANS AS A SERVICE: THE PROMISE AND PERILS OF WORK IN THE GIG ECONOMY (2018) (arguing that gig work should be regulated as other work is regulated).

[6] This Essay borrows this terminology from the Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]. Since the passage of the GDPR, "AMS" and "ADS" have become common regulatory parlance to describe different forms of automation at work.

[7] For an overview of some trends in worker surveillance related to automated decision-making systems (ADSs) at work, see IFEOMA AJUNWA, THE QUANTIFIED WORKER 75-243 (2023).

[8] *See, e.g.*, Keshav Dhir & Amit Chhabra, *Automated Employee Evaluation Using Fuzzy and Neural Network Synergism Through IoT Assistance,* 23 PERS. & UBIQUITOUS COMPUTING 43, 43 (2019); Orly Lobel, *The Law of AI for Good*, 75 FLA. L. REV. 1073, 1074 (2023).

[9] Daniel Keats Citron and Frank Pasquale have also argued that "[a]dvocates [too often] applaud the removal of human beings and their flaws from the assessment process." Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4 (2014).

[10] See, for example, Nowsta's claim that "AI empowers organizations to forecast and plan their workforce needs more accurately," *The Role of AI in Workforce Management*, NOWSTA, https://www.nowsta.com/blog/the-role-of-ai-in-workforce-management [https://perma.cc/DL4B-9JAV]; and ZenDesk's claim that "AI can improve the employee experience," Hannah Wren,

To be sure, together with appropriate legal safeguards and prohibitions, digital technology *could* be designed to help employers and workers achieve more fair, equitable, free, and democratic workplaces. To date, however, findings from sociotechnical research[11] and the cultivated expertise of workers cast doubt on the purported positive impacts of existing systems. An emergent body of empirical research on workers who are digitally managed—including research on platform workers in the logistics and transportation industries—raises serious alarms about the social, economic, psychological, and physiological harms imposed by extant forms of AMSs and ADSs.[12] Many of these harms can be understood as intensifying familiar problems. For example, research suggests that since datasets embody preexisting biases, the automated systems that rely on such data may replicate historical forms of discrimination in hiring and pay.[13] Investigations have also found that as with human oversight and evaluation, machine errors are not uncommon, but they are hard to detect and correct, resulting in erroneous, unfair evaluations and terminations with no avenue for redress.[14] Other studies observe that algorithmically determined quota systems can push

11 Ways to Use AI for a Better Employee Experience, ZENDESK (Feb. 12, 2024), https://www.zendesk.com/blog/ai-for-employee-experience [https://perma.cc/KJJ9-NJV3].

[11] Serena Oduro and Tamara Kneese argue that too often, sociotechnical research is left out of legal attempts to regulate technology. Serena Oduro & Tamara Kneese, *AI Governance Needs Sociotechnical Expertise: Why the Humanities and Social Sciences Are Critical to Governmental Efforts*, DATA & SOC'Y 1 (2024), https://datasociety.net/wp-content/uploads/2024/05/DS_AI_Governance_Policy_Brief.pdf [https://perma.cc/XB6T-C34W].

[12] *See* Collier et al., *supra* note 4, at 1-2; Jarrahi et al., *supra* note 5, at 1-6; AJUNWA, *supra* note 7, at 75-243; Citron & Pasquale, *supra* note 9, at 4; Oduro & Kneese, *supra* note 11, at 1; *see also* JULIET B. SCHOR, AFTER THE GIG: HOW THE SHARING ECONOMY GOT HIJACKED AND HOW TO WIN IT BACK 105-21 (2020) (utilizing data to review the shortfalls and potentials of "sharing platforms"); Lindsey D. Cameron, *The Making of the "Good Bad" Job: How Algorithmic Management Manufactures Consent Through Constant and Confined Choices*, 69 ADMIN. SCI. Q. 458, 461-65 (2024), https://doi.org/10.1177/00018392241236163 [https://perma.cc/K36P-4TD8] (analyzing the effects of algorithmic management and control in the workplace); KATIE J. WELLS, KAFUI ATTOH & DECLAN CULLEN, DISRUPTING D.C.: THE RISE OF UBER AND THE FALL OF THE CITY 67-87 (2023) (detailing Uber's use of data).

[13] Sarah Myers West, Meredith Whittaker & Kate Crawford, *Discriminating Systems: Gender, Race, and Power in AI*, AI NOW INST. 8-18 (2019), https://ainowinstitute.org/publication/discriminating-systems-gender-race-and-power-in-ai-2 [https://perma.cc/UAW8-WEY2].

[14] *See, e.g.*, Lauren Kaori Gurley, *Amazon's AI Cameras Are Punishing Drivers for Mistakes They Didn't Make*, VICE (Sept. 20, 2021, 9:47 AM), https://www.vice.com/en/article/amazons-ai-cameras-are-punishing-drivers-for-mistakes-they-didnt-make [https://perma.cc/FQ3Y-DCFY]; Sharon Adarlo, *There's a Problem with AI Programming Assistants: They're Inserting Far More Errors into Code*, FUTURISM (Oct. 2, 2024, 2:12 PM EDT), https://futurism.com/the-byte/ai-programming-assistants-code-error [https://perma.cc/V9CX-YQS6]. These kinds of machine mistakes and unfairness cannot be solved by just-cause regimes alone, where an employee is not supposed to be terminated from their job except with cause, absent human auditing and due process. *See infra* note 20 and accompanying text.

workers to work too hard and too quickly, resulting in serious bodily injury and offsetting the last century of occupational health and safety interventions.[15]

By and large, these researchers suggest that the intensified workplace harms caused by the introduction of AMSs and ADSs are the result of "information asymmetries" between workers and their employers.[16] Advanced AMSs invisibly enable employers to collect detailed data about workers, their movements, and their behaviors.[17] This data is then fed into ADSs – including machine-learning systems – which generate black-box rules to govern the workplace.[18] Scholars tend to assume that if workers had access to the data that is collected on them, along with knowledge of how it is used by ADSs, then they could use traditional legal avenues (for example, litigation, consultation, and collective bargaining) to challenge machine-generated mistakes and biases through the existing laws of work, just as they can challenge human-generated mistakes and biases.[19] Likewise, existing scholarship tends to assume that if workers knew and understood the algorithmic rules that govern their workplaces, they could spot and correct violations of prevailing labor and employment laws, which already protect against unsafe workplaces, identity-based discrimination, low pay, and – applicable to the European Union (EU), but not to private, nonunionized workplaces in the United States – "unjust" terminations.[20]

[15] *See generally* Veena Dubal & Vitor Araújo Filgueiras, *Digital Labor Platforms as Machines of Production*, 26 YALE J. L. & TECH. 560 (2006) (arguing that digital platforms are a new subtype of firm which may negatively impact worker health and safety).

[16] *See, e.g.*, Alex Rosenblat & Luke Stark, *Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers*, 10 INT'L J. COMMC'N. 3758, 3761 (2016) ("[T]he labor that Uber drivers do is shaped by the company's deployment of a variety of design decisions and information asymmetries via the application to effect a 'soft control' over workers' routines."). In the Spanish context, however, this "soft control" may indeed be the determining factor that makes workers "dependent." María Luz Rodríguez Fernández, *Inteligencia artificial, género y trabajo*, 171 TEMAS LABORALES 11, 32 (2023).

[17] Veena Dubal, *On Algorithmic Wage Discrimination*, 123 COLUM. L. REV. 1929, 1930 (2023).

[18] *Id.*

[19] *See* Giovanni Gaudio, Algorithmic Bosses Can't Lie! *How to Foster Transparency and Limit Abuses of the New Algorithmic Managers*, 42 COMPAR. LAB. L. & POL'Y J. 707, 733-39 (2022); Katherine C. Kellogg, Melissa A. Valentine & Angèle Christin, *Algorithms at Work: The New Contested Terrain of Control*, 14 ACAD. MGMT. ANNALS 366, 387 (2020).

[20] European Union (EU) member states use "just-cause" standards for termination; the United States does not, with the exception of the state of Montana. In the United States, the default legal standard for non-union private employment is "at will." This means that a worker can be terminated from their job at any time and for any reason, as long as it is not an illegal reason. By contrast, just-cause standards of employment are intended to prevent workers from being terminated for unfair or arbitrary reasons. Joseph A. Seiner, *Sensible Just Cause*, 103 B.U. L. REV. 1295, 1300-06, 1320-21 (2023).

Building on this research, the first wave of legislation to address the problems arising from digitalized labor control focuses almost exclusively on information transparency rights and mandates, including data access, data-processing explainability, and impact assessments. The undisputed legislative leader has been the EU. In 2018, the EU passed the first omnibus law to accord data rights to natural persons, the General Data Protection Regulation (GDPR), which has since been replicated in many jurisdictions around the globe, including in some U.S. states—most consequentially in California.[21]

Drafted primarily with consumers in mind, the GDPR also applies to workers, though comparably few have mobilized to exercise their rights under the law. More recently, in 2024, many of the rights embodied in the GDPR—including data-access rights, data-processing explainability rights, and impact assessments—were specifically mandated for platform work in the EU via the Platform Work Directive (PWD). The PWD also includes novel rights that are intended to directly address ADSs. For instance, the directive forbids platform firms from processing data on emotional, psychological, and personal beliefs, thus granting platform workers greater data-processing protections than any other workers in the EU.[22] Also in 2024, the EU passed the Artificial Intelligence Act (AI Act), which labels the workplace a high-risk setting, a designation that triggers predeployment and postmarket safeguards for employment-related AI.[23]

Together, the GDPR and the AI Act create, for the first time ever, a web of critically important—if experimental—data and data-processing rights for the work context. The PWD then builds on these rights to extend even more data protections to a subset of workers—platform workers—who are almost exclusively managed by digital machinery. As the European Commission considers the possibility of an algorithmic-management directive that would extend the rights created through the PWD to other workforces, and as jurisdictions around the world consider laws and regulations to emulate the EU legislation,

[21] California is one of eighteen U.S. states that have sought to emulate the GDPR by passing GDPR-like laws, but it is the only state to not expressly exclude workers from its coverage of data subjects. *See* California Consumer Privacy Act, 2018 CAL. STAT. 1807 (codified as CAL. CIV. CODE § 1798.100 (West 2018)); Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (July 22, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/AHQ2-FJBH].

[22] Directive 2024/2831, of the European Parliament and of the Council of 23 October 2024 on Improving Working Conditions in Platform Work, art. 7.1, 2024 O.J. at 16-17 [hereinafter PWD].

[23] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), art. 6, annex III, 2024 O.J. at 53, 127 [hereinafter AI Act].

determining the efficacy of these first-wave interventions is critical. At the time of writing, however, we still know very little about how adequately these new rights address the significant harms and problems posed by on-the-job use of AMSs and ADSs.[24]

This Essay begins to fill this gap by offering a close study of these laws, along with an analysis of a recent natural legal experiment: pioneering litigation by platform workers who exercised their data and data-processing rights under the GDPR and won access to information about termination and pay. Ride-hail workers in the EU, supported by the nongovernmental organization (NGO) Worker Info Exchange (WIE), the App Drivers and Couriers Union (ADCU), and privacy advocates, were among the first to successfully challenge a platform firm's refusal to release, in some cases, any data at all, and in others, only limited and insufficient data and data-processing information.[25] However, in an unexpected twist, the success of this litigation proves the insufficiency of current regulation.[26] While the years-long litigation led to monumental and precedent-setting judgements against ride-hail companies Uber and Ola, workers have been unable to leverage the litigation wins—and the data transparency and explanations achieved through these wins—to effect meaningful, systematic harm reduction.[27]

Through a critical analysis of this strategic litigation and the laws underpinning the litigation, this Essay argues that the first wave of data and data-processing rights for workers does not effectively address the harms arising from algorithmic management because it makes two conceptual errors. First, the laws treat workers as liberal, autonomous subjects. But by law, when people are at work, they are not free to behave autonomously. Rather, the law formally subordinates them to the firms for which they labor.[28] Arguably, then, workers'

[24] The PWD has yet to go into effect for EU member states, and mandated compliance with the AI Act is still a few years away at the time of writing.

[25] For the appellate decisions resulting from these lawsuits, see, Hof's-Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:796 (Appellants/Uber B.V.) (Neth.) (English translation of Dutch original); and Hof's-Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:804 (Appellants/Ola Netherlands BV) (Neth.) (English translation of Dutch original). *See also* Section III.A (analyzing the Uber and Ola ride-hail workers who litigated under the GDPR to address ADS problems related to pay and termination).

[26] *Id.*

[27] *Id.* Nevertheless, the released data may yet prove a useful tool of resistance: what has been released reveals an extraordinary degree of control exercised by the firms' algorithmic management systems, which will be highly consequential in the context of worker misclassification litigation for proving that the platform companies are employers.

[28] Some scholars suggest that the assumptions undergirding the GDPR, including the one that privacy and consent are the most important safeguards, are also inadequate for people acting in a consumptive capacity. *See, e.g.*, Mike Ananny & Kate Crawford, *Seeing Without Knowing:*

primary interests lie not in transparency, privacy, and consent, but in job certainty, wage security, and dignity.[29] Moreover, given the explicit legal domination afforded to employers in the workplace, laws that place the burden on workers to access and understand data-processing systems, and then to use this knowledge to circumvent present and future harms, are of limited practical utility. Low-wage workers generally lack the resources, power, and technical insight to know when their employers are not adequately complying with their obligations under data laws.

Second, by leaning primarily on transparency principles to detect, prevent, and stop violations of labor and employment laws, the GDPR, the PWD, and the AI Act do not account for the ways in which workplace algorithmic-management systems often create *new* harms that existing laws of work do not address. These harms, which fundamentally disrupt norms about worker pay, evaluation, and termination, arise from the relational logic of data-processing systems. A worker managed through or with the assistance of ADSs may not be rewarded or disciplined based on an evaluation of their individual rule compliance, productivity, and effort.[30] Rather, their intended behavioral modifications may be contextual and iterative, with variable outcomes, expectations or results based on how AMSs and ADSs understand and position them in relation to their coworkers in general and at any given time.[31] As these data-processing laws are amended and expanded in the EU and as they are considered for replication around the world—including in California and other U.S. states—legislators, workers, and worker representatives should attend to the *new* harms of algorithmic management and address the shortcomings of existing data laws.

This Essay proceeds in three Parts. Part I analyzes the GDPR, the AI Act, and the PWD specifically as laws of work and examines their principal approaches to data and data-processing rights—notice, transparency, and impact assessments—in relation to the pressing problems and precarities produced through automated labor control. Part II then positions these data laws in relation to the broader law and political economy of the workplace and argues that they do not account for workers' positionality as "illiberal" subjects—forbidden, by legal

Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability, 20 NEW MEDIA & SOC'Y 973, 979-80 (2018).

[29] For an overview of law and doctrine that govern privacy at work—and the lack thereof—see BRISHEN ROGERS, DATA AND DEMOCRACY AT WORK: ADVANCED INFORMATION TECHNOLOGIES, LABOR LAW, AND THE NEW WORKING CLASS 51-53 (2023).

[30] For example, Amazon says that it evaluates warehouse workers "in relation to how the entire site's team is performing." Jeanne Kuang, *California Hits Amazon with Fines Under Warehouse Worker Law*, CALMATTERS (June 18, 2024), https://calmatters.org/california-divide/2024/06/warehouse-workers-california-amazon-fine [https://perma.cc/3TA6-B5XX].

[31] For this understanding of algorithmic systems, I am indebted to Salomé Viljoen's insights. Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 607-16 (2021).

doctrine, from behaving in ways that are at odds with the business interests of their employers. Finally, Part III analyzes a natural experiment to extract lessons for future regulation of automated labor control. In particular, it examines the case study of Uber and Ola ride-hail workers who mobilized to vindicate their rights as data subjects under the GDPR in an attempt to address problems caused by ADSs related to pay and termination. The Essay concludes by recommending a guiding principle for future data laws, one that reflects older approaches to workplace regulation: regulation must move beyond merely elucidating and assessing data processes and shift more pointedly towards restricting the use of such data and processes where the systems cause harmful workplace outcomes.

I. THE FIRST WAVE OF DATA RIGHTS FOR WORKERS: THE EU CONTEXT

Despite the overarching data-minimization goals embedded in the GDPR,[32] digital data collection and data processing in the workplace have grown dramatically in reach and sophistication since the law's passage in 2016. From 2019 to 2022, coinciding with pandemic stay-at-home orders and new work-from-home policies, global demand for worker-monitoring software reportedly increased by sixty-five percent.[33] Across service sites and product supply chains, this intensified digital monitoring was coupled with the development of sophisticated automated decision-making software, which businesses deployed to make management decisions more rapidly, to increase production or service speed and scale, and to lower labor overhead.[34]

Firms that self-identify as "platforms"[35] and use what scholars have called a "platform management model"[36] were among the first to experiment with what is now called "algorithmic management" – the automation of work processes and management functions, including coordination and control of a workforce, often

[32] The GDPR's data minimization principle can be found in Article 5.1(c): "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')." GDPR, *supra* note 6, at 37, art. 5.

[33] Danielle Abril, *Your Boss Can Monitor Your Activities Without Special Software*, WASH. POST (Oct. 7, 2022), https://www.washingtonpost.com/technology/2022/10/07/work-app-surveillance [https://perma.cc/D3L2-AXLE].

[34] *Id.*

[35] As Vitor Filgueiras and I have argued, these are not fundamentally new types of firms, but rather firms that use new technologies to control their workforce. *See* Dubal & Filgueiras, *supra* note 15, at 565-66.

[36] Phoebe V. Moore & Simon Joyce, *Black Box or Hidden Abode? The Expansion and Exposure of Platform Work Managerialism*, 27 REV. INT'L POL. ECON. 926, 926 (2020).

via machine-learning systems.[37] But the techniques of digitalized workplace surveillance and algorithmic management first observed in "platform work" were quickly adopted by firms with more traditional employment models.[38] Accordingly, extant research on platform work is particularly useful for understanding trends in algorithmic management across the labor market.

Two particularly significant forms of algorithmic management, which this Essay uses to ground its analyses of existing data laws, are the uses of ADSs (1) to set wages (sometimes through the allocation of work or wage products) and (2) to evaluate and terminate workers. Through automated wage-setting practices, known in the platform-work literature as algorithmic wage discrimination, firms use social data[39]—including data extracted from workers' labor—to "personalize and differentiate wages for workers in ways unknown to them, paying them to behave in ways that the firm desires, perhaps for as little as the system determines that the workers may be willing to accept."[40] While algorithmic wage discrimination—the transference of consumer price discrimination to the work context—was first documented in on-demand work, traditional employers have also commenced using machine-learning software to "tailor each employee's compensation" in ways that remain opaque to the workforce.[41] Similarly, "deactivation," a euphemism for termination engineered by on-demand firms, has traveled to more traditional employment settings in which automated decision-making software is now used to invisibly and opaquely evaluate and dismiss workers, even in just-cause jurisdictions.[42]

[37] Jarrahi et al., *supra* note 5, at 1.

[38] *Id.* at 2.

[39] Drawing on Salomé Viljoen and Elettra Bietta's work, I use the term "social data" rather than "personal data" to underscore the degree to which data used by firms to analyze, understand, predict, and influence human behaviors only makes sense when thought about relationally, not through the lens of a single individual, but through how that individual's personal data relates to another person's or population's personal data. In that sense, the kinds of data I am concerned about in the Essay are in fact better understood as social data. *See* Viljoen, *supra* note 31, at 607-16; Elettra Bietta, *Data Is Infrastructure* 2-3, THEORETICAL INQUIRES IN L. (forthcoming 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5041965 [https://perma.cc/C2HV-L2WG].

[40] Dubal, *supra* note 17, at 1935.

[41] *See, e.g.*, *AI in Compensation and Benefits: Predictive Analytics*, HRBRAIN.AI (Jan. 29, 2024), https://hrbrain.ai/blog/ai-in-compensation-and-benefits-predictive-analytics [https://perma.cc/P7FF-QHT3] (describing the use of artificial intelligence (AI) predictive analytics to set compensation for individual workers).

[42] In just-cause jurisdictions, employers cannot fire workers unfairly or arbitrarily. *See supra* note 20 and accompanying text. For more on technologically enhanced performance monitoring, see Valerio De Stefano, *"Negotiating the Algorithm": Automation, Artificial Intelligence, and Labor Protection*, 41COMPAR. LAB. L. & POL'Y J. 15, 23-24 (2019). For more on deactivation problems faced by workers who labor for platforms, see *Fired by an App: The Toll of Secret Algorithms and*

Both automated wage-setting and automated evaluation/termination systems create novel harms and new logics of labor control, often allowing firms to hew to the letter of existing employment laws while evading their spirit. For example, in low-wage sectors, hourly wages are conventionally transparent to individual workers, certain, and set by individual or collective contracts. Though performance-based variable pay using offline evaluation processes and bonus structures is not uncommon, wage discretion is limited by laws that protect workers from discrimination based on protected identities and those that create minimum-wage and overtime-wage floors.[43] Variable pay and discipline practices, even in the at-will employment context, typically operate through norms and logics that associate hard work, rule-following, and worker loyalty with higher pay and work security.[44] But the novel logics of some data-processing systems, discussed further in Part II, disrupt these norms and introduce new experiences of uncertainty to the workplace, thereby unsettling the relationship between work and economic security.

Just as concerns about data and data-processing in the consumer context have largely focused on safeguarding individual data privacy and consent, concerns about data and data-processing in the workplace have focused centrally on transparency, to the detriment of other principles like fairness and economic security.[45] According to the prevailing view among analysts, from which this Essay departs, the central problem with algorithmic management is that workers governed by such systems lack knowledge about the basic rules they must follow. In contrast to labor process customs of nondigital, offline scientific management, in which workers are typically informed of workplace expectations,[46] workers

Unchecked Discrimination on California Rideshare Drivers, ASIAN AMS. ADVANCING JUST. & RIDESHARE DRIVERS UNITED (Feb. 2023), https://www.advancingjustice-alc.org/media/Fired-by-an-App-February-2023.pdf [https://perma.cc/2MLM-GWLC].

[43] Dubal, *supra* note 17, at 1957-61. Work *hours* are often unpredictable – sometimes set by just-in-time systems – but payment for hours worked is more reliable. For more on the instabilities associated with just-in-time scheduling, see Joshua Choper, Daniel Schneider & Kristen Harknett, *Uncertain Time: Precarious Schedules and Job Turnover in the US Service Sector*, 75 ILR REV. 1099, 1102-05 (2022).

[44] This is because in offline variable pay, employees act as stakeholders in firm productivity; they are paid more for adhering to employer rules and working toward incentives. According to Lisa A. Burke and Chengho Hsieh's review of the management science literature, "[Offline] variable pay can lead to an increase in motivation and employee performance. This is largely due to the incentive effect that variable pay has on employee behavior." Lisa A. Burke & Chengho Hsieh, *Optimizing Fixed and Variable Compensation Costs for Employee Productivity*, 55 INT'L J. PRODUCTIVITY & PERFORMANCE MGMT. 155, 157 (2006).

[45] This, of course, is not to undervalue privacy for workers. For more on how data analytics can intrude on worker privacy and the repercussions, see De Stefano, *supra* note 42, at 27.

[46] As I have shown elsewhere, the founder of scientific management theory, Frederick Taylor, believed that the production of knowable rules through management science would create

are left to wonder: How are their wages determined? In what ways are they being evaluated and by what metrics? What is the world of behaviors that might lead to discipline or termination? Knowing what data is being extracted and understanding the logic behind the ADSs, observers argue, would enable workers to adjust to the digital labor processes and to address violations of existing labor laws. Following this reasoning, legislative authorities in a few jurisdictions, including in some U.S. states and in the EU, have moved to create transparency rights for workers or to extend existing data-transparency rights to the workplace.

In the following Sections, I examine the most prominent of these data laws in the EU – specifically, laws embodied in the GDPR, the AI Act, and the PWD – and analyze how they attempt to address the problems raised by algorithmic labor control. I focus on these laws because they, and in particular the GDPR, have become global models for workers' data- and digital-protection laws.[47] For example, the California Privacy Rights Act (CPRA), which is the most expansive and developed data-rights law for workers in the United States, is explicitly modelled on the GDPR. The EU, meanwhile, may soon consider adopting another algorithmic-management directive modeled after the PWD but applicable to all workers.

A. *The General Data Protection Regulation (2016)*

The GDPR, the first broadscale law governing data privacy for "natural persons," went into effect in May 2018 and imposes "obligations onto organizations anywhere [in the world], so long as they target or collect data related to people in the EU."[48] In practice, the GDPR creates regulations "on the usage, storage and movement of data."[49] While the GDPR's emphasis on making data usage explainable to natural persons is primarily aimed at allowing consumers to make informed decisions about the data collection and data processing to which they

workplace democracy. "Taylor's primary contention was that through the effort to maximize efficient production, rules became knowable – to both workers and their bosses. Workers would know what was expected of them and could, in theory, use a 'code of law' developed through scientific management to justify complaints to management." Dubal, *supra* note 17, at 1965.

[47] *See, e.g.*, Anis Bajrektarevic & Valentina Carvajal Caballero, *GDPR as a Global Model for Data Protection–Analysis*, EURASIA REV. (Oct. 17, 2024), https://www.eurasiareview.com/17102024-gdpr-as-a-global-model-for-data-protection-analysis [https://perma.cc/6NBF-93JX].

[48] Ben Wolford, *What Is the GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr [https://perma.cc/RG6Q-NWLF].

[49] Gerard Buckley, Tristan Caulfield & Ingolf Becker, *GDPR: Is It Worth It? Perceptions of Workers Who Have Experienced Its Implementation*, ARXIV 2 (2024), https://arxiv.org/pdf/2405.10225 [https://perma.cc/8TYN-DRNV].

consent,[50] these obligations can also be leveraged by workers who, by law, have very few privacy rights in the workplace. Even though "opting out" or refusing to consent to a data-processing system at work is effectively impossible without exiting a job, the GDPR provisions could, observers argue, at least help workers to understand how they are monitored and managed.[51]

The GDPR is a regulation, not a directive, which means that except in very specific instances, EU member states were required to adopt it into national law without changes.[52] However, member states were allowed to modify how the law applied to employment, a formal recognition of the distinctive nature of work.[53] Article 88, which governs data-processing rights in employment, gives significant leeway to each member state to adopt their own laws with regard to the "data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the *transparency* of processing [and] the *transfer* of personal data."[54] Member states developed a patchwork of data-processing laws in response to Article 88, with varying degrees of protection for workers,[55] though

[50] GDPR regulators have made the law's consumer focus clear. The EU's online guide to GDPR compliance states: "The GDPR installs a new, basic contract between the companies and the consumers." *What Does the GDPR Mean for Business and Consumer Technology Users*, GDPR.EU, https://gdpr.eu/what-the-regulation-means-for-everyday-internet-user [https://perma.cc/F9N3-PESQ].

[51] *See, e.g.*, Hannah Johnston & M. Silberman, *Using GDPR to Improve Legal Clarity and Working Conditions on Digital Labour Platforms: Can a Code of Conduct as Provided for by Article 40 of the General Data Protection Regulation (GDPR) Help Workers and Socially Responsible Platforms?* (Eur. Trade Union, Working Paper No. 2020.05, 2020), https://www.etui.org/publications/using-gdpr-improve-legal-clarity-and-working-conditions-digital-labour-platforms [https://perma.cc/G2KH-RG2X].

[52] *See Types of Legislation*, EUR. UNION, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en [https://perma.cc/LL9X-6R46] ("A 'regulation' is a binding legislative act. It must be applied in its entirety across the EU.").

[53] GDPR, *supra* note 6, at 86, art. 88.1 ("Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.").

[54] *Id.* (emphasis added). In the EU, "fundamental rights" are broadly construed but framed through liberal, not material, principles. They are dignity, freedom, democracy, equality, rule of law, and respect for human rights, including those of minorities. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

[55] Halefom H. Abraha, *A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace*, 12 INT'L DATA PRIV. L. 276, 280-83 (2022).

these laws all reflect the GDPR's general approach to workers' data rights as articulated in Recital 4, which is to find a balance between an employer's right to monitor their employees in the workplace and the employee's right to privacy in the workplace.[56] On its face, this approach pits the ideal of worker "consent"—once informed about data collection and data-processing, workers are free to exit the job—against the employers' "legitimate interests." It also neglects other worker interests, including economic security, with the unstated assumption that those interests are adequately addressed through the existing laws of work, including minimum-wage and just-cause regulations. However, as developed in Part II, given the legal deference to the managerial or employer prerogative, "consent" to workplace monitoring provides only a facade of privacy protections for workers who must work to live.

To date, the primary rights under the GDPR that have been utilized by workers and their representatives to gain transparency over data collection and automated decision-making systems are outlined in Articles 15, 20, and 22. On their face, these Articles allow workers to obtain their data and to understand the logic of the data-processing rules that algorithmically control them. However, even though personal data collected by employers are essentially valueless to workers in the absence of insight into why they are being collected and how they are being used,[57] some employers have taken the position that the release of firm logics undercuts the competitive advantages created through algorithmic labor control.[58] Consequently, while employers have been more forthcoming in releasing (at least some) personal data, they have been more reticent to release the logic of their data-processing systems.[59]

Nevertheless, the GDPR does mandate this kind of logic transparency.[60] Articles 15 and 22, most critically, give workers the right to know the rules of the workplace—to understand the automated systems that are used to evaluate their labor, determine their wages, discipline them, and terminate their

[56] Eddie Keane, *The GDPR and Employee's Privacy: Much Ado but Nothing New*, 29 KING'S L.J. 354, 359-63 (2018).

[57] Jathan Sadowski, Salomé Viljoen & Meredith Whittaker, *Everyone Should Decide How Their Digital Data Are Used—Not Just Tech Companies* 595 NATURE 169, 170 (2021).

[58] This has been litigated under EU competition law. For more, see Miranda Cole & Francesco Salis, *Evolving View of Data in the Application of Competition Law*, GCR (May 17, 2024), https://globalcompetitionreview.com/guide/data-antitrust-guide/first-edition/article/evolving-view-of-data-in-the-application-of-competition-law [https://perma.cc/WDH6-TWCE].

[59] *See, e.g.*, Natasha Lomas, *Uber Still Dragging Its Feet on Algorithmic Transparency, Dutch Court Finds*, TECHCRUNCH (Oct. 5, 2023, 11:00 AM PDT), https://techcrunch.com/2023/10/05/uber-slow-on-algo-transparency [https://perma.cc/4C9C-SVYC].

[60] *See infra* Table 1 for a summary of key data rights afforded to workers under the GDPR.

employment—and to contest the misapplication of these rules.[61] Article 15 guarantees natural persons, including workers, the right to be informed about the existence of automated decision-making and to be provided with meaningful information about the logic by which these systems process their data.[62] As a complement to this transparency mandate, Article 22 effectively provides workers with the right to have a "human in the loop" when decisions being made have legal or significant effects.[63] The plain text of Article 22 mandates that while firms can rely on evaluations from ADSs to make workplace decisions—like terminations—that have significant effects on workers, they cannot rely *solely* on those systems.[64]

Article 20, meanwhile, gives workers the right to receive the personal data concerning themselves and the right to data portability. Article 12 requires such data to be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[65] However, though many workers have requested their data under Article 20, the data they receive is often practically meaningless to them without further processing or visualization, and advocates argue that the companies "frequently omit the data categories most conducive and necessary for interrogating the conditions of work."[66] Given the obfuscating nature of digital systems, it is nearly impossible for workers (and regulators) to know whether the information requested has been properly made available. For example, in 2019, Uber provided telematic data in response to data-subject access requests, but they stopped doing so in 2020 and 2021.[67] Workers who sought this data were left to wonder whether Uber had stopped collecting this safety data, or whether they just refused to release it to drivers for inspection.[68] Without a full-scale public auditing of Uber's systems, it is impossible to know.

Beyond the enumerated rights listed in Articles 15, 20, and 22, Article 35 of the GDPR contains another important safeguard against excessive monitoring

[61] GDPR, *supra* note 6, at 45, 48, arts. 15, 22.

[62] *Id.* at 45, art. 15.

[63] *Id.* at 22, art. 22; *see also* Talia Gillis, *Regulating for "Humans-in-the-Loop,"* ECGI BLOG (Sept. 27, 2022), https://www.ecgi.global/publications/blog/regulating-for-humans-in-the-loop [https://perma.cc/DT5J-WLPQ] (describing Article 22 as a requirement for a "human-in-the-loop").

[64] GDPR, *supra* note 6, at 22, art. 22.

[65] *Id.* at 41-42, art. 12.

[66] Cansu Safak & James Farrar, *Managed by Bots: Data-Driven Exploitation in the Gig Economy*, WORKER INFO EXCH. 43 (2021), https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_8d720d54443543e2a928267d354acd90.pdf [https://perma.cc/X4P6-YK9U].

[67] *Id.* at 67.

[68] *Id.*

of natural persons.[69] The Article mandates that firms acting as data controllers carry out Data Protection Impact Assessments (DPIA) prior to processing personal data, if the processing is "likely to result in a high risk to the rights and freedoms of natural persons."[70] In the case of employment, however, this requirement has had little bite: though ADSs that process personal data often pose such consequential risks to workers, rarely are such impact assessments carried out or made public. One reason may be that firms narrowly interpret "personal data" to exclude "de-personalized" banded or grouped data derived from personal data.[71] For example, a firm like Uber might repurpose personal data related to how often a worker rejects a ride to train machine-learning systems on what rides to allocate to that worker and when. But the ADSs that allocates the work might be using banded data, in which that worker is included in a subset of similarly behaving workers. Thus, a firm may decide that since only data *derived* from personal data is used to train the machine-learning system, a DPIA is not required for that system.[72] Another limitation of Article 35 is the lack of guidance on what constitutes an adequate assessment. As Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, and Madeleine Clare Elish have written, "What counts as an adequate assessment, when that assessment happens, and how stakeholders are made accountable to each other are contested outcomes shaped by fraught power relationships."[73] This is a particularly salient concern for the workplace.

Since the implementation of the GDPR, many of the rights enumerated by these Articles have been undermined in practice. In some cases, firms have released the data to workers in non-machine-readable formats, making it impossible to analyze even when workers partner with data analysts.[74] In other cases, definitional ambiguities have prevented workers from gaining the insights that

[69] GDPR, *supra* note 6, at 55-56, art. 35.

[70] *Id.*

[71] *See id.* at 35, art. 4(1) (defining personal data as "any information relating to an identified or identifiable natural person" and an identifiable natural person as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, [or] an online identifier"). In contrast, banded or grouped data is organized into categories rather than attributable to individual persons.

[72] EU privacy advocates contest this interpretation of GDPR obligations. Author's Fieldnotes (Feb. 2024) (on file with author).

[73] Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh & Madeleine Clare Elish, Algorithmic Impact Assessments and Accountability: The Co-Construction of Impacts 2 (ACM 2021 Conf. on Fairness, Accountability, and Transparency, Feb. 12, 2021), https://ssrn.com/abstract=3736261 [https://perma.cc/V8TK-WU8U].

[74] Safak & Farrar, *supra* note 66, at 43.

they need.[75] Companies have also frequently argued that releasing the data-processing logic is tantamount to releasing "trade secrets," or that doing so would harm the security of others.[76] In the absence of affirmative litigation—which requires substantial resources that most workers lack and puts workers at risk of retaliation—workers who dare exercise their rights must accept whatever data firms provide to them.

TABLE 1. SUMMARY OF KEY DATA RIGHTS AFFORDED TO WORKERS UNDER THE GDPR

Relevant GDPR Articles	Data Rights Accorded to Workers
88	Extension of the GDPR to employment settings, with leeway granted to Member States to provide more specific rules.
15	The right to know whether or not personal data concerning the worker is being processed and, where that is the case: The right to access personal data and the following information: the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; The right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; The right to lodge a complaint with a data controller; The right to know where the personal data is collected if it is not collected from the data subject; The right to know about the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the worker.
20	Right to portability: to receive personal data that the firm has provided to a data controller.

[75] For example, workers have been terminated for their "fraud probability" score, but "fraud" as used by the companies does not necessarily meet the definition of criminal or civil fraud. Instead, it may be a firm-specific use that reflects something about performance management or evaluation. *See id.* at 22-30.

[76] See, for example, Uber's argument in the litigation described *infra* Section III.A.2.

Relevant GDPR Articles	Data Rights Accorded to Workers
22	Right not to be subject to a decision that is based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects them. This is sometimes interpreted by firms as being a mandate to have a "human in the loop."
35	In the context of high risks to the rights and freedoms of national persons and when a type of processing in particular uses new technologies, the right, prior to the processing, to have a data controller carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

B. The Artificial Intelligence Act (2024)

The AI Act, at the time of writing, is the newest of the European laws to safeguard against the potential impacts of AI systems.[77] The Act follows a "risk-based approach," reinforces GDPR data rights, and creates some new transparency and assessment mandates for the use of AI at work.[78] In contrast to the GDPR, which places the burden on the worker to invoke their "right to know"[79] when automated decision-making systems are being used, the AI Act directs employers to inform workers and workers' representatives affirmatively that they are subject to these AI systems.[80] But this affirmative duty does not include any requirement to explain the workplace rules or systems logics that are embedded

[77] The AI Act defines "AI system" as

> a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

AI Act, *supra* note 23, at 46, art. 3.

[78] *Id.* at 7, pmbl., para. 26.

[79] GDPR, *supra* note 6, at 12, pmbl., para. 63.

[80] AI Act, *supra* note 23, at 67-68, art. 26. Specifically, the Preamble of the AI Act proposes that the risks associated with AI in employment are as follows:

> AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions *affecting terms of the work-related relationship*, promotion and termination *of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics* and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons *and workers' rights*.

Id. at 16, pmbl., para. 57 (emphasis added).

in the AI, thus leaving workers in the dark about how their pay is determined, how they are evaluated, when they might be disciplined or terminated, and other consequential impacts of these systems. Together with the exercise of rights in Articles 15 and 22 of the GDPR, the knowledge that an employer is using AI systems may be useful during collective bargaining, but for the roughly seventy-seven percent of nonunionized workers across the EU member states, the notification by itself does little to curb any subsequent harm.[81] Again, the underlying principle of this provision is one of consent: once a worker is informed of the use of the AI system, they are free to exit the job; if they stay, they are acquiescing to being subject to and managed by AI. For many low-wage, economically precarious workers, however, the exit option is illusory, and it becomes ever more limited as workplaces increasingly utilize machine-learning systems for labor management.

More promisingly, the Preamble of the AI Act outright bans the production and use of AI that emotionally manipulates people

> to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making, and free choices . . . whereby significant harms, in particular having sufficiently important adverse impacts on . . . financial interests are likely to occur.[82]

The application of this prohibition to the employment context remains unclear. This prohibition could be interpreted to ban some of the interactive systems that on-demand algorithmic-management companies use to allocate work and determine pay.[83] For example, if firms treat their workforce as self-employed (a problem addressed by the PWD[84]), then perhaps AI systems used to nudge workers to accept work that they would not otherwise accept and to prod them to move to places they would not otherwise move may be affirmatively prohibited.[85] But in the context of legally recognized formal employment, such systems produced

[81] *See* Ethan Dazelle, *A Closer Look: Labor-Management Cooperation in Europe*, U.S. DEP'T. LAB. BLOG (May 2, 2024), https://blog.dol.gov/2024/05/02/a-closer-look-labor-management-co-operation-in-europe [https://perma.cc/62PA-QT58] (discussing labor-union density in the EU).

[82] AI Act, *supra* note 23, at 8, pmbl., para. 29.

[83] *See, e.g.*, Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. TIMES (Apr. 2, 2017), https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html [https://perma.cc/BXX8-648B] (discussing how Uber uses interactive features to control workers' behavior).

[84] *See infra* Section I.C.

[85] *See* Scheiber, *supra* note 83 (discussing Uber's features that encourage drivers to move "where Uber wants them to go").

by the employer would likely be protected by the managerial prerogative.[86] In those contexts, the AI would likely be treated as high-risk but not prohibited entirely.[87]

Indeed, the AI Act considers the use of most AI in the employment context to be unambiguously high-risk, an implicit recognition of the economic dependency on employment for survival and of the doctrinal implications of the managerial prerogative.[88] The Act divides firms into "providers" and "deployers."[89] Employers who purchase AI to use on their workforce—the deployers—have limited obligations under the Act. Most of the regulatory onus falls on the providers of AI. Specifically, in recognition of the iterative and changing nature of machine-learning systems, the AI Act mandates that providers of AI that is developed for hiring, performance, management, and monitoring—including software that sets wages, evaluates, and disciplines workers—must develop a risk-management system by August 2026, when the regulation comes into force.[90] This system must include testing mandates[91] that follow a product through its life cycle, including in its post-market phase when the product is purchased and used by a deployer (the system is thus reliant on compliance by deployers with monitoring and reporting obligations).[92] Providers must specifically examine how the system is "likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under [EU] law."[93]

Responsibility for evaluation, recordkeeping, testing, and risk assessment likewise falls primarily on the provider, not on the deployer or on an unbiased, public third party.[94] Instead of directly mandating public assessments of these

[86] *See infra* Section II.A.

[87] The preamble to the AI Act states: "[I]t is appropriate to classify [AI systems] as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence." AI Act, *supra* note 23, at 14, pmbl., para. 52. As defined in Annex III of the AI Act, high-risk systems include those used in employment and workers' management. *Id.* at 127-29, annex III. AI systems deemed high-risk are subject to more obligations before being put on the market and used. *Id.* at 56, art. 9.

[88] *See infra* Section II.A.

[89] AI Act, *supra* note 23, at 46, art. 3.

[90] *Id.* at 56, art. 9; *id.* at 123, art. 113.

[91] *Id.* at 57, art. 9.

[92] *Id.* at 56, art. 9; *see also id.* at 101, art. 72 (laying out the requirements for post-market monitoring).

[93] *Id.* at 57, art. 10.

[94] *Id.* at 56, art. 8. The Act requires deployers to follow the instructions of the providers, guarantee some human oversight, validate input data, monitor AI systems' activity and report problems to the providers, and save logs if possible. *Id.* at 59-60, art. 13.

systems at the deployment level, as would be ideal, the Act requires self-regulation by the firms that create the machine-learning systems, who are required to maintain human oversight and monitoring for specific issues – most relevant here, violations of the EU's Fundamental Rights and the health and safety of workers.[95] But the Act provides no guideline for evaluating harms related to the workplace. How is a provider to test for "health and safety" impacts? What are the criteria to evaluate a system that creates low and unpredictable wages in relation to worker health and safety? Does the emotional distress caused by an AI system that invisibly evaluates workers make the system "unsafe"? These are questions that remain unanswered. As with the GDPR, the lack of clear guidelines around harm and fairness calls into question the efficacy of these life-cycle assessments, even if they are carefully and inclusively conducted.[96]

C. *The Platform Work Directive (2024)*

While the GDPR and the AI Act offer rights to workers of all stripes, the PWD explicitly emphasizes that the rights it enumerates apply only to platform workers, who are granted more expansive data and data-processing rights than any other workers in the EU.[97] "Platform work" is defined narrowly as "a form

[95] If a private entity is using AI to provide public services (including transportation), the rules are slightly different. Article 27 of the AI Act requires that these entities must do their own impact assessment to make sure no fundamental rights are being violated. *Id.* at 69, art. 27. This might include a private employer that is contracted by a city to provide transportation or construction services. Notably, it does not require the hiring entity to ensure the systems do not violate existing employment laws or pose problems for the health and safety of workers who are interacting with the AI systems. For purposes of oversight, the Act mandates that providers of high-risk AI systems must automatically maintain logs of such AI system for six months – a paltry amount of time in the context of potential litigation. *Id.* at 64, art. 19. On its own, the AI Act does not adequately address any of the harms that research has documented is experienced by workers who are surveilled and controlled at work through AI systems. For example, the Act would not affirmatively stop the use of AI systems that produce variable pay, which I have documented as causing harm to workers. *See* Dubal, *supra* note 17, at 1976-92.

[96] For example, research by Uber's chief economist in collaboration with other analysts found that Uber drivers who are women earn lower hourly wages than men, even controlling for the times they drive. They attributed this to, among other things, "the logic of compensating differentials (and the mechanisms of surge pricing and variation in driver idle time)." *See* Cody Cook, Rebecca Diamond, Jonathan V. Hall, John A. List & Paul Oyer, *The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers*, 88 REV. ECON. STUDS. 2210, 2211 (2021). But, if surge pricing and work allocation are determined by Uber's AI systems, would this mean that Uber, as a provider and deployer in a high-risk context, must stop using these systems? What if the systems only *contribute* to disparate impacts on protected categories of people? On its face, the AI Act does not answer these questions.

[97] PWD, *supra* note 22, at 3, pmbl., para. 14.

of employment in which organizations or individuals use an online platform to access other organizations or individuals to solve specific problems, or to provide specific services in exchange for payment."[98] At the time of writing, though the PWD has passed the EU Parliament, it has not been put into effect by member states.[99] Thus, the analysis in this Section is speculative; nevertheless, this directive is particularly useful to evaluate because, compared to the GDPR and the AI Act, the PWD provides broader and arguably more-effective rights to a specific subset of workers who are subject to ADSs and AMSs.[100] Unlike the two previously discussed bodies of legislation, the PWD was written with platform workers in mind and more expansively addresses the problems they face.[101]

Specifically, the PWD offers "more specific safeguards concerning the processing of personal data by means of automated systems in the context of platform work" and recognizes that "the consent of persons performing platform work to the processing of their personal data cannot be assumed to be freely given."[102] Unlike both the GDPR and the AI Act, the PWD reaches beyond transparency, consent, and impact assessments to affirmatively prohibit the use of certain processing of personal data relating to the individual's body, mental state,

[98] *EU Rules on Platform Work*, EUR. COUNCIL (Oct. 16, 2024), https://www.consilium.europa.eu/en/policies/platform-work-eu [https://perma.cc/FK97-VNHQ] (emphasis omitted).

[99] Following the European Council's adoption of the PWD in October 2024, member states have two years to incorporate the PWD into their national legislation. *Id.* For more problems with the PWD and specific policy recommendations to broaden its effect, see Silvia Rainone & Antonio Aloisi, *The EU Platform Work Directive: What's New, What's Missing, What's Next?*, EUR. TRADE UNION INST. (Aug. 6, 2024), https://www.etui.org/sites/default/files/2024-08/The%20EU%20Platform%20Work%20Directive-what's%20new%2C%20what's%20missing%2C%20what's%20next_2024.pdf [https://perma.cc/PB4A-TNTV].

[100] PWD, *supra* note 22, at 22, pmbl., para. 8 ("Persons performing platform work [who are] subject to . . . algorithmic management often do not have access to information on how the algorithms work, which personal data are used or how the behaviour of those persons affects decisions taken by automated systems . . . . Moreover, persons performing platform work often do not know the reasons for decisions taken or supported by automated systems and are not able to obtain an explanation for those decisions, to discuss those decisions with a human contact person, to contest those decisions or to seek rectification or, where relevant, redress.").

[101] *See supra* note 97 and accompanying text.

[102] PWD, *supra* note 22, at 7-8, pmbl., paras. 38-39. These prohibitions include those on "process[ing] any personal data on the emotional or psychological state of persons performing platform work . . . [or] in relation to their private conversations, collect[ing] any personal data while persons performing platform work are not offering or performing platform work, process[ing] any personal data to predict the exercise of fundamental rights, . . . [or] process[ing] personal data to infer the person's racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, . . . emotional or psychological state, trade union membership, sex life or sexual orientation." *Id.* at 8, pmbl., para. 40.

protected identity, or personal beliefs.[103] These are not full-scale prohibitions, however. For instance, the PWD may permit automated processing if the data is depersonalized through banding, a loophole that could affect groups of workers exercising their fundamental rights, including their freedom of association.[104] Moreover, while it bans the processing of biometric data, it allows "biometric verification" such as the use of facial recognition technologies to identify workers, even though such systems have a higher false-positive rate for people of color and can lead to unfair termination.[105]

The PWD may also fail to attend to the structural realities of digital control. Critically, the PWD does not affirmatively prohibit automated decision-making in contexts related to hiring, pay determination, work allocation, discipline, and termination.[106] Instead, it extends the rights embedded in Article 35 of the GDPR to the context of platform work by mandating that firms carry out impact assessments before new ADSs are deployed.[107] Such firms must "carry out a data-protection impact assessment" to evaluate the impact of ADSs' processing of personal data on the rights and freedoms of persons performing platform work.[108] The firms' assessment must be carried out every two years and shared with workers and workers' representatives.[109] One problem with this approach, however, is that by allocating the responsibility for this evaluation to the firms themselves (as opposed to mandating a public audit), the PWD, like the AI Act, neglects the enforcement problems that arise with black-box systems. Given the competitive incentives for firms to maintain secrecy around these systems, how does a worker or workers' representative know that the impact assessment includes all the AMSs and ADSs that the firm deploys?

A second and more significant problem is that like the GDPR, the PWD fails to lay out meaningful standards or criteria for the impact evaluations of the ADSs or affirmative steps that must be taken if the ADSs are found to be harmful. The

[103] *Id.*

[104] *Id.*

[105] *Id.* at 8, pmbl., para. 41. In 2018, Joy Buolamwini and Timnit Gebru published findings that three commercial face-recognition systems had a higher rate of false positives for women with darker skin, largely because of the training data the models used. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77, 87-89 (2018). Soon thereafter, Microsoft & IBM determined to improve their systems, but errors remain. *See* Abeba Birhane, *The Unseen Black Faces of AI Algorithms*, NATURE (Oct. 27, 2022), https://www.nature.com/articles/d41586-022-03050-7 [https://perma.cc/WUW7-4XGQ].

[106] PWD, *supra* note 22, at 7-8, pmbl., para. 38.

[107] *Id.* at 8, pmbl., para. 43.

[108] *Id.*

[109] *Id.* at 9, pmbl., para. 47.

presumption embedded in the PWD is that if the assessment finds that the evaluated systems detrimentally impact workers' fundamental rights or violate the labor laws of a particular member state, the firm will then refrain from deploying the system. But many of the harms experienced by platform workers – including those that arise from algorithmic wage-discrimination practices and automated termination practices – do not necessarily violate any existing fundamental rights or the labor rights enumerated by member states. For example, if an ADS uses personal data to determine a worker's wages, as long as the wages do not fall below the minimum wage and as long as they do not differentially impact workers based on protected identities, they are not per se unlawful under existing employment laws. Indeed, even though such algorithmic wage discrimination has clearly identified harms to workers – such as increasing income uncertainty[110] and workforce division[111] – an impact assessment by a platform company is not likely to capture these harms or consider them when deploying the systems, in large part because they serve the firm's profit interests.

The PWD also contains transparency obligations in relation to AMSs and ADSs used by the platform company. On their face, these obligations are stronger than those embodied in the GDPR because they place an affirmative obligation upon the platform companies rather than relying on workers to exercise these rights. Per the directive, platform companies must provide information to workers

> in relation to automated monitoring systems and automated systems which are used to take or support decisions that affect persons performing platform work, such as . . . their access to . . . work assignments, their earnings, their safety and health, their working time . . . , their promotion or its equivalent, and their contractual status, including the restriction, suspension or termination of their account.[112]

This may not only force firms to make their algorithmic logics public, but also make the implications of such systems the subject of public debate and contention. Still, the nature of machine-learning systems puts this outcome in question.[113]

Though the PWD has yet to be adopted by member states, we can make some predictions about its effects. First, because the PWD extends greater digital

[110] *See* Dubal, *supra* note 17, at 1969-75.

[111] One of the biggest problems of differential wages or tiered wage systems is their negative impact on worker solidarity. *See* Veena Dubal, *The New Racial Wage Code*, 15 HARV. L. & POL'Y REV. 511, 518-26 (2021).

[112] PWD, *supra* note 22, at 8, pmbl., para. 44.

[113] *See infra* Section II.B.

rights to "platform workers" than to other workers, the directive may invite firms to engage in definitional arbitrage not only with respect to whether their workers are "employees" but also as to whether they themselves are "platform companies," thus undermining the potential impact of the law's assessment and transparency obligations. Second, even assuming proper classification, there is reason to be concerned about the directive's ability to curb harms caused by ADSs. As the case studies discussed in Part III show, transparency and information-sharing on their own are not immediately useful in the context of a workplace in which digital systems are constantly changing and in which firms rely on these systems to create competitive market advantages.

The most promising parts of the PWD are its outright prohibitions, not only because they affirmatively protect workers from technologies currently causing extensive harms across the EU, but also because they gesture toward the possibility of an alternative approach to ADSs and AMSs in which data laws reach beyond transparency to focus on direct harm avoidance. Indeed, an absolute ban on certain data-processing systems may be appropriate when the outcome of deploying such systems is likely to be fundamentally at odds with fair, equitable, and secure work. This idea is further developed in Part III.

TABLE 2. SUMMARY OF KEY DATA RIGHTS AFFORDED TO WORKERS UNDER THE PWD

Relevant PWD Articles	Data Rights Accorded Platform Workers
7	Limitations on the processing by means of AMSs and ADSs of (1) personal data related to the emotional or psychological state of the person performing the platform work; (2) personal data related to private conversations; (3) personal data to predict the exercise of fundamental rights; (4) personal data to infer racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, including chronic disease or HIV status, the emotional or psychological state, trade union membership, information about a person's sex life or sexual orientation; (5) biometric data to establish a person's identity by comparing that data to stored biometric data of other individuals. Limitations on the collection by means of AMSs and ADSs of personal data of a person while that person is not offering or performing platform work.
8	Mandated data-protection impact assessment when processing of personal data by a platform by means of AMSs and ADSs is likely to result in a high risk to the rights and freedoms of natural persons. These assessments must be provided to workers' representatives.

Relevant PWD Articles	Data Rights Accorded Platform Workers
9.1	Digital labour platforms must inform workers and their representatives of the use of AMSs and ADSs. Information should include the types of decisions supported by ADSs. As to AMSs, that information should specifically include the fact that the systems are in use or are in the process of being introduced, the categories of data and actions monitored, the aim of the monitoring and how it is achieved, and the recipients of the personal data collected (including if it is transmitted or transferred within a group of undertakings). As to ADSs, that information should include that such systems are in place or being introduced, the categories of decisions that are taken or supported by the decisions, the categories of data and the main parameters that such systems take into account and the relative importance of those parameters, and grounds for decisions to restrict, suspend, or terminate the account of a worker, and to refuse the payment for work performed.
9.2	All the above information should be in a written document, presented in transparent, intelligible and easily accessible form.
9.3	Workers should receive concise information about the systems that affect them, including their working condition, at the latest on the first working day. They should be informed of any introduction of changes. Upon request, they should be provided with detailed and comprehensive information about relevant systems and their features.
9.4	Prior to the use of those systems or to the introduction of changes that affect working conditions, workers' representatives should be provided with detailed and comprehensive information about relevant systems and their features.
9.5	Platforms must provide the information specified above to persons undergoing a recruitment or selection process.
12	In consultation with workers and/or their representatives, firms must evaluate the risks of AMSs and ADSs to worker safety and health and introduce appropriate preventative and protective measures. They cannot use ADSs and AMSs to put undue pressure on workers or put their physical and mental health at risk.
23	Workers who have been terminated for exercising the above rights in the Directive may request the firm to substantiate the termination in writing.

II. WORKPLACE SUBORDINATION AND THE NEW LOGICS OF WORKPLACE CONTROL

> They are using Big Data as a replacement for the Big Boss.
>
> – California-based Uber Driver[114]

Though welcome, the first wave of EU digital rights discussed above does not adequately address many of the harms specific to new forms and logics of automated labor control. In large part, as I discuss below, this is because the digital rights offered by these legislative initiatives – even the PWD – make a critical category error. They treat workers in the same way that they treat consumers: as liberal subjects whose primary interests are in privacy, consent, and transparency. But people work to live – to purchase necessities like shelter and food – and thus have a unique dependency on their employers. This economic dependency is compounded by the fact that in many legal systems, including in the EU and the United States, workers are not treated as autonomous equals when they are on the job; they are, by law, subordinated to their employer.[115] The primary interests of workers, then, may be better understood as wage security, job certainty, and on-the-job dignity. The question then becomes: do data rights laws help workers to achieve these central interests?

As discussed below, in critical ways, data-processing systems may change the entire premise of workplace control, making collective knowledge of the rules embedded in the data-processing systems largely unhelpful to workers. Instead of operating through systems of clear, fixed rules and progressive discipline procedures in which workers are evaluated individually (as has been the norm under a previous generation of scientific management), firms that rely upon automated data-processing systems may control workers by situating them relationally to one another, creating iterative rules based on evaluation of the entire workforce. Evaluation, then, is collective and contextual, and may operate to continually modify worker behavior. Indeed, workers' knowledge of the logic of the ADSs may even compel a race to the bottom, prompting them to behave in self-exploitative ways. As discussed herein, the legal subordination and dependency of workers, combined with the relational logic of data-processing for workplace

[114] Author's Fieldnotes (Feb. 2024) (on file with author).

[115] For information on the managerial or employer prerogative in U.S. law, see Gali Racabi, *Abolish the Employer Prerogative, Unleash Work Law*, 43 BERKLEY J. EMP. & LAB. L. 79, 87-92 (2022). For more information on the employer prerogative in the European Union, see Mia Rönnmar, *The Managerial Prerogative and the Employee's Obligation to Work: Comparative Perspectives on Functional Flexibility*, 35 INDUS. L.J. 56, 61-69 (2006).

control, inhibit the capacity of transparency, assessment, and consent mechanisms to create workplaces with certainty, security, and dignity.

A. *Workers as Illiberal Subjects*

Workers are, by law and circumstance, necessarily subordinated to their employers. Unlike "natural persons" in the larger polity—who, as consumers or even as citizens, can make basic demands of a firm or of the state without fearing economic or (ideally) political repercussions—workers are not empowered to behave independently of their employer's interests. This means that, as a practical matter, rights to gain insights into the algorithmic logics of management are difficult for workers to exercise. And even when workers find a way to exercise such rights (as demonstrated by the litigation case studies in Part III), without powerful independent worker representation, such as through a union or NGO, it is nearly impossible for individual workers to make sense of the data released, ensure the information is comprehensive, or bargain over the terms of the AMSs and ADSs. The PWD directly encourages this kind of collective consultation in the narrow case of platform work, but it also presupposes the existence of such independent, representative bodies—which, in many cases, do not exist.[116]

The fact that employees (or workers functionally treated like employees) are legally subordinated to their employers is not solely, or even primarily, a product of the contractual specifications that govern any particular employment relationship. Rather, it follows from the legal doctrines that constitute employment. In contrast to most civil or commercial contractual relationships, the employment relationship is predicated on the prerogatives of the employer. The employer has—within certain legislatively inscribed or collectively bargained-for legal bounds—the unfettered discretion to control and direct the worker on the job (and sometimes, particularly as it relates to speech, off-the-job activities as well).[117] Unless otherwise contracted for, an employer can control when a

[116] As Sylvia Rainone and Antonio Aloisi write, "Article 15 stipulates that only providers with worker status have the right to be assisted by representatives in monitoring the impact of AM on working conditions (Article 10(1)), to take part in risk assessments of occupational safety and health (Article 12(2)) and to exercise information and consultation rights on the introduction of, or substantial changes in the use of, automated monitoring and decision-making (Article 13)." In these contexts, representative bodies—unions or nongovernmental organizations—can assist workers in asserting their rights and consult on the introduction of new automated monitoring systems (AMSs) and ADSs. Rainone & Aloisi, *supra* note 99, at 7. For more on the collective consultation rights embedded in the PWD, see MARÍA LUZ RODRÍGUEZ FERNÁNDEZ, LABOUR LAW AND DECENT WORK IN THE PLATFORM ECONOMY (forthcoming 2025).

[117] Together, the doctrine of the managerial prerogative and the common-law control test for employer/employee relationships solidify a legal framework in which workers are subject to

worker uses the bathroom, when they eat a snack, what they wear, and how they behave.

Empirical analysis has shown that even in the setting of "platform work" – where the companies dispute the classification of their workers as employees, and in most jurisdictions legally treat them as self-employed (an issue that the PWD separately addresses[118]) – firms have used the doctrine of managerial prerogative to confer a general prerogative of enterprise ownership.[119] That is, they have maintained both that their workers are not employees *and* that despite this, the managerial prerogative allocates them the right to exert labor control.[120] Uber, for example, maintains that as owners of enterprise, they can use digital technologies to coordinate labor operations, and that they do not need to be considered employers to do so.[121] Workers for Uber, meanwhile, have little control over labor operations beyond when they begin and end their shifts, yet are denied the labor-law protections normally afforded to employees.[122]

The doctrine of the managerial prerogative is legally and ideologically reinforced in most U.S. and EU jurisdictions by versions of the common-law agency test that determines who is an employee.[123] Though the specifics of this test vary by jurisdiction, most jurisdictions recognize that to benefit from employment and labor rights, the hiring entity must exert a high degree of control over "the manner and means" of how the work is conducted.[124] Different versions of this test and different judicial approaches do not necessarily reflect a broad consensus of what "control" looks like – especially in digitalized labor control.[125] Nevertheless, the underlying assumption is clear: employers have the presumed legal authority to "control" (or in the civil-law context, "subordinate") the worker and the workplace,[126] making the individual exercise of transparency rights difficult and risky.

what philosopher Elizabeth Anderson calls "private government." ELIZABETH ANDERSON, PRIVATE GOVERNMENT: HOW EMPLOYERS RULE OUR LIVES (AND WHY WE DON'T TALK ABOUT IT) 41 (2017).

[118] PWD, *supra* note 22, at 15-16, arts. 3-5.

[119] Julia Louise Tomassetti, *Managerial Prerogative, Property Rights, and Labor Control in Employment Status Disputes*, 24 THEORETICAL INQUIRIES L. 180, 180 (2023).

[120] *Id.* at 181.

[121] *Id.* at 186.

[122] *Id.*

[123] *Id.* at 183.

[124] *Id.*

[125] *Id.* at 184.

[126] *Id.*

In light of workers' relative powerlessness in the workplace, their constant fear of termination, the risk of disciplinary repercussions,[127] and the limited impacts of the rights themselves on workplace harms, workers are unlikely to individually exercise their digital rights to request data transparency or request access to or challenge the scope and validity of impact assessments. In the EU, unlike in the United States, workers labor under a default regime of just-cause protections—meaning they cannot be fired except for "just cause"—and thus cannot legally be fired merely for exercising their data rights.[128] But even with such protections, the introduction of automated termination systems and enshrouding of workplace rules with algorithms make it difficult for workers to ascertain and contest pretextual termination, absent due process.[129] Thus, not only are workers' primary interests not directly represented by the existing web of data rights, but these data rights are also conceptually limited by the legal structures of employment such that they are inadequate vehicles for helping workers to achieve certainty, security, and dignity in the workplace.

B. From Individual to Relational Control

> Data access can pour petrol on the fire. It confirms for us what our own intuition says is happening [in terms of how we are controlled]. But let's not kid ourselves. We understand the logic and then the rule changes.
>
> —James Farrar, United Kingdom-based former Uber driver[130]

In the collective context, transparency mechanisms may in theory empower workers to exercise their existing rights. For example, if the ADSs were allocating wages that fall below legislated minimum-wage standards, then transparency laws like those embedded in the GDPR and the PWD may be useful in holding

[127] Among existing laws for worker data protection, only the PWD, which has not yet gone into effect in the EU, contains an affirmative protection against retaliation. "Member States shall introduce the measures necessary to protect persons performing platform work . . . from any adverse treatment by the digital labour platform and from any adverse consequences resulting from a complaint lodged with the digital labour platform or resulting from any proceedings initiated with the aim of enforcing compliance with the rights provided for in this Directive." PWD, *supra* note 22, at 23, art. 22.

[128] *See supra* note 20 and accompanying text.

[129] Further, automated monitoring and algorithmic management have also expanded the scope of what might constitute cause. With on-demand ride hail work, for example, workers have been terminated for "fraud." But what constitutes "fraud" is firm-specific and does not necessarily correlate with commonly understood notions of fraud. *See supra* note 75 and accompanying text. Under a union contract, some of these things (though not all) could become the subject of negotiation with workers' representatives.

[130] Author's Fieldnotes (Feb. 2024) (on file with author).

the employer to the letter of the law and deterring them from non-compliance. However, in many cases, mere knowledge about algorithmic-management systems will not enable workers to understand or effectively negotiate workplace control, nor will such knowledge necessarily help workers to overcome new harms arising from control enacted through machine-learning systems. These failures are related. Not only are many of the problems posed by digitalized control new and unaccounted for by the existing panoply of work laws, but the systems of control themselves also depart from more familiar forms of scientific management. Rather than a definitive set of rules knowable to the employer and the employee, the iterative use of algorithms and data means that workplace rules for control are ever-shifting—aimed at dynamic behavior modification and instrumentalization.

Under traditional models of scientific management, worker efficiency and productivity are created through cognizable forms of rulemaking and application.[131] Rules are generated through a careful analysis of work processes, with the aim of eliminating temporal and material inefficiencies in production and lowering labor overhead.[132] Employers convey the rules to workers whose individual jobs include completion of one or more components of the production process.[133] Workers are then individually evaluated by human managers for compliance with those rules.[134] Workers who comply with rules keep their job; workers who violate rules lose their jobs or are otherwise disciplined.[135] Ideally, workers who excel in compliance with workplace rules advance in their jobs and are rewarded with higher wages.[136] As sociologist Michael Burawoy long ago observed, these approaches to worker control emphasize rule "compliance and obedience to management in the pursuit of a common interest."[137]

Under workplace management that takes place through machine-learning systems, however, these logics and norms are disrupted: the rules are mutable, wages are not necessarily tied to individual rule compliance, and hard work may become technically disentangled from advancement and higher wages.[138]

[131] *See supra* note 46 and accompanying text.

[132] *See* FREDERICK WINSLOW TAYLOR, THE PRINCIPLES OF SCIENTIFIC MANAGEMENT 9-28 (1919).

[133] *Id.* at 36.

[134] *Id.* at 70.

[135] *Id.* at 124-25.

[136] *Id.* at 94.

[137] Michael Burawoy, *Toward a Marxist Theory of the Labor Process: Braverman and Beyond*, 8 POL. & SOC'Y 247, 279 (1978). Burawoy also points out that by trying to create a common intersect between employers and employees, scientific management was an "ideological attack on the nascent trade union movement" of the industrial revolution. *Id.*

[138] Dubal, *supra* note 17, at 1959.

Employers still break down processes and create foundational rules for each component of the work process with the goals of increasing production and decreasing labor costs. AMSs collect personal data on individual workers' on-the-job behavior, and employers may purchase data about workers' off-the-job and previous job behavior (including, possibly, where they live, how much they have historically been paid, and so on).[139] This data—constantly collected—is fed into algorithmic systems that then train computers, iteratively creating new rules of workplace control. These dynamic rules aim to change the behavior of individual or banded workers.[140]

The iterative customization of management to modify worker behavior, however, qualitatively changes the mode of production, particularly the relationship between worker rule compliance and labor costs. Employers no longer have to decrease labor costs through temporal efficiencies gained by direct rule compliance by workers. For example, algorithmic systems can be used to minimize labor costs through the personalization of worker wages.

Thus, not only does the nature of algorithmic management make it impossible for workers to behave in ways that pave opportunities for advancement, but, based on machine-learning analysis and decisions, workers may also be differentially treated and paid, from moment to moment and from day to day. For example, while traditional models of scientific management include ascribing a fixed hourly wage to a given job, algorithmic management frequently uses dynamic wages (or "wage manipulators") that seek to modify worker behavior.[141] On one day, they may earn higher wages. On the next day, despite doing all the same things they did the day before, they may earn less. Evaluations are not necessarily made individually, based on a single worker's behavior, but contextually, based on the worker's behavior in relation to the population of other workers. Collectively understanding the logic of the decision-making systems, then, will not necessarily help workers to excel in their jobs, because the system may be designed to learn about and categorize behaviors and treat individuals or groups of workers differently, relative to each other.

Thus, automated data-processing systems may make unpredictability and uncertainty standard features of work. For instance, in contrast to offline management systems, algorithmic management systems will not necessarily reward loyalty and hard work—indeed, under such dynamic systems, it may not be possible to know what constitutes hard work. The relational logic of the systems

[139] *Id.* at 1946.

[140] *Id.* As Fourcade and Healey write in *Ordinal Society*, "The rules of the game are unclear, and they adjust dynamically, whether it is as a response to new information or to allow for the myriad of experiments always running in real time." MARION FOURCADE & KIERAN HEALY, THE ORDINAL SOCIETY 250 (2024).

[141] For more on wage manipulators, see Dubal, *supra* note 17, at 1949.

both complicates the definition of hard work and makes it a moving target. As Uber's own research suggests, for example, drivers who labor for longer periods of time typically earn less per hour.[142] Likewise, leaked corporate documents about Amazon's warehouse labor management reveal that workers are terminated when automated systems determine that their productivity levels fall to the bottom twenty-five percent.[143] This means that workers can be fired not just for violating known workplace rules, but also for performing in ways that position them as perceived outliers in dynamic, digitalized productivity evaluation.[144] The workplace rules no longer create a "common interest" between the employer and the worker, as Burawoy observed.[145] Instead, the workers' interest may become disconnected from the employer's, severing the norms that used to connect workplace obedience and rule compliance with worker security.

III. THE FAILURES AND FUTURES OF DATA LAWS AS WORK LAWS

> [N]o employer has given a full and proper account of the automated personal data processing. . . . This is a tool of resistance rather than [merely] a tool of retrieving information.
>
> – Cansu Safak, Worker Info Exchange Research Lead[146]

One reason platform work has served as a laboratory for algorithmic management systems is that many firms that use platforms to control their workforces also maintain that those workers are self-employed.[147] To maintain this facade, the firms have experimented with different forms of digitally enabled

[142] Cody Cook, Rebecca Diamond, Jonathan Hall, John A. List & Paul Oyer, *The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers* 3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 24732, 2018).

[143] Colin Lecher, *How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity*,' VERGE (Apr. 25, 2019, 12:06 PM EDT), https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations [https://perma.cc/X8Y6-HF6W].

[144] One advocate shared with me that workers who plucked feathers off chickens in a factory in Los Angeles County were given "wearables" to evaluate how quickly and how well they did their job. But prior to the introduction of the wearables, workers had developed their own plucking techniques. The digital evaluation could not capture these individually varied techniques and thus did not accurately judge their productivity. Author's Fieldnotes (Feb. 2024) (on file with author).

[145] Burawoy, *supra* note 137, at 273.

[146] Author's Fieldnotes (Feb. 2024) (on file with author).

[147] Dubal, *supra* note 17, at 1946.

labor control.[148] In addition to framing rules as "suggestions," firms using platforms to manage their workforce might use the opacity and uncertainty of their pay, work allocation, and termination systems to compel workers into behaving in certain (sometimes self-exploitative) ways.[149] Firms may use "wage manipulators," such as surge pricing or bonus incentives, to compel workers to labor at certain times and for longer periods of time.[150] They may use "algorithm updates" to alter worker behavior or to change how the firm distributes work and determines pay.[151]

In this context, platform workers have discovered the importance of having and understanding their data, which, at a minimum, can help them articulate why they should benefit from existing employment and labor law protections. In this Part, I examine the first strategic litigation of workers under the GDPR to gain access to their data and to the underlying logic of the data-processing systems that determine their pay and work allocation and flag them for suspension or termination. As discussed below, despite the successful litigation, access to such information has not had the kinds of impact that workers had hoped. Still, the litigation may be critical to establishing employment status and building on-the-ground resistance amongst an already-distressed workforce. And, perhaps most importantly, this strategic litigation illuminates the path that future legislation on data rights at work should take. Prospective legislation must not only tackle the barriers to transparency revealed through these cases, but it must also proscribe outcomes and algorithmic systems that undermine the basic interests of workers.

A. Strategic Litigation to Mobilize Data-Processing Rights for Workers

In 2016, James Farrar (alongside his coworker Yaseen Aslam) sued Uber, alleging that the company misclassified them as self-employed workers.[152] After five years of litigation, the U.K. High Court agreed.[153] But at the tribunal level, Uber argued that Mr. Farrar was not owed work protections because they allowed him to behave like a small businessperson; they did not even discipline

[148] Alex Rosenblat & Luke Stark, *Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers*, 10 INT'L J. COMMC'N 3758, 3759 (2016).

[149] *Id.* at 3762-77.

[150] *Id.* at 3762; Dubal, *supra* note 17, at 1949.

[151] Dana Calacci, *Organizing in the End of Employment: Information Sharing, Data Stewardship, and Digital Workerism*, MIT MEDIA LAB (2022), https://www.dcalacci.net/papers/211.12.10-calacci-chiwork-latest.pdf [https://perma.cc/4BY5-8AYK].

[152] Aslam v. Uber B.V. [2016] EAT 1, [12] (Eng.).

[153] Uber BV v. Aslam [2021] UKSC 5, [2] (appeal taken from Eng.).

him for declining a large percentage of rides.[154] As an example, Uber showed that on week 27 on the job, he had worked for 91 hours, refusing 60% of rides sent to him. Mr. Farrar, flummoxed by this information and his memory of how hard he worked, located the "on-boarding document" that Uber had provided to him when he was hired.[155] The document indicated that workers were expected to do 1.4 to 1.5 trips per hour to be considered productive, far less than he had completed.[156] "This," Mr. Farrar said, "[m]ade me understand that I needed to control my own data to [be able to prove I was] an employee."[157]

Mr. Farrar went on to establish the Worker Info Exchange (WIE), a public-interest nonprofit in the European Union, with the mission of supporting platform workers in "navigating this complex and under regulated space."[158] Using the GDPR, WIE has made "data subject access requests" and "data portability" requests on behalf of individual workers to help them understand terminations or why their accounts have been flagged for fraudulent activity.[159] In some instances, though making the request has been "extremely time consuming and capacity intensive," they have enabled individual workers to get their jobs back.[160] However, these requests, on their own, do not address the broader problems and harms of algorithmic management—the use of the automated systems that caused their terminations in the first place. Perhaps more alarmingly, WIE has found that "companies have shown a tendency to deny the data practices they do not wish to disclose."[161]

WIE has also pursued strategic litigation that challenges the responses of specific companies to their data subject access requests. This litigation, which focused on the algorithmic control practices of the ride-hailing firms Uber and Ola, sought to learn how the companies allocated work, determined pay, assessed performance, and terminated workers—all of which, though basic aspects of work, were shrouded by firms. Exercising collective digital rights under the GDPR, WIE, working alongside the App Drivers and Couriers Union (ADCU) in the United Kingdom, represented eleven drivers based in the United

[154] Aslam v. Uber B.V. [2016] EAT 1, [61]-[66] (Eng.); Author's Fieldnotes (Feb. 2024) (on file with author).

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] Safak & Farrar, *supra* note 66, at 7. Until the Worker Info Exchange, workers were not aggressively using their GDPR rights or challenging the data releases they received when they did exercise their rights. "You don't use it, you lose it. So, we make sure workers use it," Mr. Farrar said of the GDPR. Author's Fieldnotes (Feb. 2024) (on file with author).

[159] Safak & Farrar, *supra* note 66, at 69.

[160] *Id.* at 54.

[161] *Id.*

Kingdom, the Netherlands, and Portugal seeking access to data, algorithmic transparency, and algorithmic protection from automated decision-making. In both cases, the workers won access to the information on appeal. Below, I analyze these cases and discuss the limitations of the GDPR data rights they successfully leveraged.

1. *Ola Cabs: Transparency to Understand Termination*

In June 2020, on behalf of three drivers who had been terminated by Ola, WIE and ADCU filed collective data requests under Articles 15, 20, and 22 of the GDPR.[162] Using language from Ola's privacy policy, WIE focused on requesting the drivers' "fraud probability score" that Ola indicated that they relied upon, the "earning profile" of the workers, and the logic of work allocation.[163] The drivers hoped to gain access to their own trip and transaction data so that they could check their payment calculations over time, and to better understand the automated decision-making relevant to work allocation, performance management, and dismissals.[164] The workers also alleged, under Article 22, that they had the right to a human in the loop—to not be subject to automatic decision-making that "significantly affect[s]" the data subject.[165]

After WIE and ADCU's initial victory against Ola for lack of compliance, the company appealed the lower court decision.[166] Broadly, the appeal concerned (1) whether the automated decision-making triggered legal consequences for drivers or otherwise "significantly affect[ed] them," which would mean that the ADSs would be subject to the data release, (2) whether Ola could lawfully invoke an exception to not comply with the request, and (3) if the data to be shared under the GDPR was indeed "personal data."[167] The Amsterdam Court of Appeal ruled largely in the workers' favor, finding that the ADSs that produced the "fraud probability score," "earning profile," and journey allocation all fell under Article 22 and "significantly affect" the workers whose jobs were impacted by

[162] Rb.-Amsterdam 3 november 2021, C/13/689705 (Applicants/Ola Netherlands BV) (Neth.) (English translation of Dutch original).

[163] *Id.* As Mr. Farrar stated, "Part of the problem is that we don't know what they have, so we don't know what to ask for. The court says [the drivers] have to somehow be specific in what they are asking for." Author's Fieldnotes (Feb. 2024) (on file with author).

[164] Rb.-Amsterdam 3 november 2021, C/13/689705 (Applicants/Ola Netherlands BV) (Neth.) (English translation of Dutch original).

[165] *Id.*

[166] Hof's-Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:804 (Appellants/Ola Netherlands BV) (Neth.) (English translation of Dutch original).

[167] *Id.*

these ADSs.[168] The decision referenced the European Data Protection Board Guidelines, which specify that Article 22 cannot be circumvented by a firm's "feigning" human intervention.[169] "To achieve genuine human intervention," the court wrote, "the controller must ensure that any oversight of the decision-making process is meaningful and not merely symbolic," and "[a]s part of its data protection impact assessment, the [data] controller must identify and record the extent of human intervention in the decision-making process and the stage at which it took place."[170] Ola argued that the relevant question under the GDPR is whether automated decision-making takes place "on the basis of" the fraud probability score.[171] The court, however, held that the question was whether the score itself is "based exclusively on automated processing," because the score had significant legal effects on the driver.[172] The same was said about the drivers' "earning profiles" and allocation of journeys.[173]

The court also rejected Ola's claims that the information requested contained trade secrets regarding its business model and security measures taken by the company, as it found that the company had failed to substantiate these claims.[174] Regarding explainability of the automated decision-making, the court wrote, "The information provided must be sufficiently complete for the data subject to understand the reasons for the decision . . . [but] it does not necessarily have to be a complicated explanation of the algorithms used . . . ."[175] Ola's initial response had thus been noncompliant with the GDPR because it was too brief and general. The company was subsequently ordered to communicate "the most important assessment criteria and their role in the automated decisions," so that drivers could not only understand how decisions are made but also check the correctness of the systems as to their own work.[176]

Despite the success of the workers' appeals, the data transferred by Ola to WIE has been, in the words of one advocate, "horse shit."[177] This is due not only to the tremendous amount of analysis that must be done to make sense of the data, but also because of the relational nature of these data-processing systems described above. The rules and logic of pay and termination have also changed

[168] *Id.*

[169] *Id.* at ¶ 3.4.

[170] *Id.*

[171] *Id.* at ¶ 3.43.

[172] *Id.* at ¶ 3.42.

[173] *Id.*

[174] *Id.* at ¶¶ 3.46-47.

[175] *Id.* at ¶ 3.48.

[176] *Id.* at ¶ 3.7.

[177] Author's Fieldnotes (Feb. 2024) (on file with author).

since workers first filed their claims three years prior to the appellate decision. And, as in other instances, critical rules and explanations seem to have not been shared or released. For example, Ola explained how they allocated work to drivers as follows:

> We use a combination of customer and driver personal data, such as: . . . booking cancellation history, booking acceptance history, distance from user, home location preference, payment method preference, fuel type of the car, lease details of vehicle, car maintenance history, proximity to customer, fraud probability score, [and/or] interaction history with customer care . . . to allocate drivers' vehicles to requesting customers, and to determine the route and pricing.[178]

How are each of these factors valued and weighed? How can a worker use this information to make it more likely that they will be allocated good work? What else falls in the "such as" category? Without a public audit of Ola's systems, the workers have no way of comparing what they were able to obtain from this successful litigation to the systems that Ola uses to verify their intuitions about how the systems might work.

Even with access to the data and the technical ability to analyze it, workers will remain at a fundamental disadvantage because firms that use ADSs and AMSs can quickly change their systems, undermining whatever knowledge workers might gain through transparency rights. Moreover, even if a worker has access to data collected on them and theoretically is also granted access to the logic of algorithms, translating that information into an understanding of how those algorithms affect their working conditions is not a simple or straightforward matter. Algorithms do not function like offline workplace rules. How does a worker translate the logic of an algorithm from the viewpoint of the firm to the experience of the worker? Is an algorithm that determines the allocation of bonuses as wage manipulators to incentivize a worker to work longer hours good or bad? Is it the bonuses that augment worker stress, or does stress arise from the algorithmic allocation of those bonuses—disseminating them in different amounts to different workers at different times? It is nearly impossible for workers to use the algorithmic information provided to them to identify or isolate the precise cause of their workplace harms.

[178] *How We Process Your Data*, OLA (July 20, 2018), https://www.olacabs.com/tnc?doc=ola-privacy-policy-uk-data-processing [https://perma.cc/4M3H-428M].

2. *Uber: Transparency to Understand Pay and Work Allocation*

WIE also represented a group of eight Uber drivers in making another data-subject access request. Under GDPR Article 15, they requested a variety of information on data and automatic decision-making systems, this time related to how drivers are allocated work and paid.[179] This information included requests to access the logic of Uber's "batched matching system" (used to allocate work by matching drivers and passengers) and "upfront pricing system" (used to differentially determine base wages for each trip).[180]

Like Ola, Uber initially shared an insufficient set of data. When challenged in court,[181] the company argued that the information requested contained trade secrets, and that providing it "could lead to circumvention of those processes [by drivers] and [also that] competitors could take advantage of it."[182]

Appropriately, the Amsterdam Court of Appeal rejected Uber's defense. Taken as a whole, the court found that these systems "affect[] [the drivers] to a considerable extent" and that such impacts on workers outweighed the company's trade secrets claim; thus, under the GDPR, the company was obligated to explain systems of work pay and work allocation to workers.[183] Although this case was decided in April 2023, as of this writing, Uber has yet to provide adequate information to the drivers. Instead, they have paid a high penalty to the workers for failing to comply with the order.[184]

Uber's defense in this instance may also help us understand the limitations of transparency. Uber argued essentially that by *knowing* the rules of the workplace, workers could circumvent the management systems.[185] On its face, this defense reveals the extent to which their system of control relies not just on opacity but on ADSs that situate workers in relation to one another asymmetrically.

[179] Safak & Farrar, *supra* note 66, at 71-72.

[180] *Id.*

[181] Hof's-Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:796 (Appellants/Uber B.V.) (Neth.) (English translation of Dutch original).

[182] *Id.* at ¶ 3.38.

[183] *Id.* at ¶¶ 3.33, 3.39.

[184] "The companies have been given two months to provide the requested information to the drivers (with the risk of fines of daily several thousand euros apiece for non-compliance), as well as being ordered to pick up the majority of the case costs." Natasha Lomas, *Drivers in Europe Net Big Data Rights Win Against Uber and Ola*, TECHCRUNCH (Apr. 5, 2023, 9:22 AM PDT), https://techcrunch.com/2023/04/05/uber-ola-gdpr-worker-data-access-rights-appeal [https://perma.cc/R5VG-VGRR]. According to James Farrar, workers have received money for Uber's failure to comply.

[185] Hof's-Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:796, ¶ 3.38 (Appellants/Uber B.V.) (Neth.) (English translation of Dutch original).

Knowledge of the algorithmic logic might advantage one worker over the other by allowing him to behave in ways that send him more work at higher wages; but because the system works relationally, if *all* workers had this knowledge and behaved accordingly, the managerial logic would be disrupted.

In this Uber case, as in the Ola case, workers were successful in leveraging their data rights because they acted collectively through the protection of both a union and a nonprofit. Not only did this enable them to make the initial data-subject access request, but it also empowered them to challenge the paucity of the companies' release through litigation. Despite the landmark wins in both cases, workers were unable to change, circumscribe, or otherwise address the harms that emerged from the data collection and automated decision-making. Merely gaining access to the data and, in the case of Ola, to an explanation of the logics of pay and termination, has done little to stop what workers perceive to be arbitrary and abusive terminations and suspensions.[186] Nor has it enabled them to overcome algorithmic wage discrimination, which has created unequal, uncertain pay for equal work.[187]

This is not to say, however, that these cases are unimportant for workers. As WIE points out, their significance is not so much in the details of what has been released, but in understanding that a high degree of control is exerted using automated systems. Making this kind of control visible—for example, by showing the nature of what leads to automated driver termination and the consequences of this kind of automation—helps establish that drivers' on-the-job behavior is highly controlled and thus supports the claim that drivers should be eligible for employment protections. So, too, may these cases and their outcomes help build on-the-ground labor movements to contest the ways in which algorithmic management systems have disrupted workplace norms and, in particular, the connection between long, hard work and economic security.

B. *Proscriptive Approaches to Digital Labor Control*

What can we glean from the limitations of this first wave of data and data-processing laws? This Essay's close study of the GDPR, the AI Act, and the PWD, alongside its close analysis of WIE's successful, strategic litigation, reveal some key takeaways that may be useful to legislators or regulators seeking to expand data rights for workers.

One set of lessons applies directly to how future data laws may be crafted with an eye towards addressing the asymmetrical legal relationship between workers and their hiring entities. Data transparency should be a set of affirmative

[186] Dubal, *supra* note 17, at 1969-76.

[187] *Id.*

obligations of hiring entities, not, as per the GDPR, a right extended to workers that they must proactively operationalize themselves. Moreover, the entity using the algorithmic systems (not just the entity that produced them, as with the AI Act) should be required to carry out periodic impact assessments throughout the lifecycle of the systems. Finally, the data-processing systems used to digitally control workers should also be subject to periodic public or third-party audits in order to promote comprehensive compliance. Failure to comply adequately with data obligations should prompt not just state action but also private enforcement, a possibility currently precluded under some data-privacy laws, including the CPRA.

Future legislation should also address the myriad ways in which firms attempted to evade WIE's data-access and explainability requests. Data releases must be made in ways that are machine-readable for ease of analysis by workers and their representatives. "Personal data" must be affirmatively broadened by statute to include all social data (such as banded or grouped data) that is derived from personal data, even if not clearly traceable to an individual. So, too, must legislation proactively address evasive legal arguments related to third-party safety and trade-secret claims to facilitate expeditious sharing of information. Merely stating, as the GDPR does, that trade-secret defenses should not necessarily inhibit data access requests is insufficient.

The final and most critical lesson derived from this analysis is that data transparency and even periodic, publicly available, and contestable impact assessments might not subvert some of the new harms created through algorithmic management systems. Given the nature of machine-learning systems and the threats that they pose to job security, wage certainty, and dignity at work, legislators concerned about automation at work should focus on the systems' outcomes.

Traditional employment law does more than improve procedure and promote transparency: it provides substantive protections. Indeed, traditional employment law affirmatively safeguards the specific interests of workers in health, safety, security, and dignity by proscribing certain firm behaviors. It does not just require firms to pay workers, but rather affirmatively bans wages that fall below a minimum. And it does not just require firms to tell workers how dangerous a machine is, but instead creates standards for machine use to ensure human safety. Moving forward, as legislators seek to regulate algorithmic management, they can and should build more substantive protections.[188] As algorithmic

[188] An excellent example of legislation that did attempt to address machine-learning systems that set iteratively evaluated quotas for warehouse work is California's AB-701. Sometimes referred to as the Amazon Warehouse Law, this law requires that employers provide workers with written quota expectations upon hiring. And if those expectations change, workers must be informed within 30 days. The bill was passed to address the fact that due to AMSs and ADSs,

labor management further disrupts the normative connection between work, dignity, and economic security, some practices can and should be affirmatively redlined. For example, ADSs should not be allowed to set wages, determine the rules for termination, or terminate workers. Rather than merely governing the data, legislators should aspire to govern the *use* and *outcome* of data and data processes.

CONCLUSION

> Data [transparency] rights can be part of a movement building model. You're building worker knowledge, and workers make it part of their campaign. . . . [T]his is a continuous process, which unions have to be a part of . . . . It's part of building worker power.
>
> —James Farrar, Former Uber Driver, Founder of Worker Info Exchange[189]

As discussed above, the most prominent and far-reaching data laws for workers have originated in the EU. However, as these laws were modeled on and followed laws addressing problems faced by consumers, they tend to make faulty assumptions about the nature of the digital workplace. In placing a high value on transparency and algorithmic explainability, the laws presuppose that if a worker understands the rules embedded in the algorithmic management systems by which they are hired, paid, evaluated, disciplined, and terminated, then the online workplace is no different from the offline workplace. This assumption fails to account for the formal, legal subordination of workers to their employers—a subordination that makes full exercise of these rights difficult. Critically, it also misunderstands the nature of algorithmic labor management. Unlike traditional scientific management systems in which rule transparency creates the possibility of worker compliance, algorithmic labor control makes obfuscation

Amazon workers suffered nearly twice the serious injury rate of other warehouses. Wire Service, *Protecting Amazon Workers: The Relevance of AB 701 for the Bay Area and Beyond*, S.F. EXAM'R (Sept. 28, 2021), https://www.sfexaminer.com/news/protecting-amazon-workers-the-relevance-of-ab-701-for-the-bay-area-and-beyond/article_9d962b24-38b0-5c42-90ae-41be618a68fd.html [https://perma.cc/WUV6-FKX4]. Almost years after the law's passage, the California Labor Commissioner fined Amazon $5.9 million dollars for violating this law. But Amazon cleverly maintains that the ADS it uses does not set "quotas" but instead conducts (shifting and relational) individual performance evaluations. As one worker put it, "They keep us in the dark about our rates for the day, and they write us up when we miss the mysterious targets." Leticia Jones, *Amazon Fined $5.9 Million Dollars for Allegedly Violating California's Warehouse Quota Law*, ABC NEWS (June 19, 2024), https://abc7.com/post/amazon-fined-59-million-allegedly-violating-californias-warehouse/14972284 [https://perma.cc/3XKP-ECEM].

[189] Author's Fieldnotes (Feb. 2024) (on file with author).

of the rules a necessary part of the labor-management process. That is, algorithmic management works, in part, by evaluating workers dynamically in relation to each other, through a set of constantly changing, iterative rules.

As evidenced by the case studies discussed in this Essay, even knowing the basic logics of such a system does not necessarily help workers with rule compliance, as they are not judged individually but in relation to one another. Thus, while transparency of workplace rule logics and the privacy of workers are certainly important policy outcomes, they are insufficient by themselves for protecting workers. ADSs that result in new workplace practices and harms—like algorithmic wage discrimination and automated termination—should be addressed affirmatively through legislation that emulates more traditional, proscriptive laws of work. To this end, this Essay concludes that data laws focused on the workplace must affirmatively proscribe—not merely elucidate—these forms of worker control.

Professor of Law, University of California, Irvine; Postdoctoral Fellow, Stanford University; Ph.D. 2014, University of California, Berkeley; J.D. 2006, University of California, Berkeley School of Law; B.A. 2003, Stanford University. The author profusely thanks the many scholars and advocates whose thinking, feedback, and conversation informed this Essay. These people include but are not limited to María Luz Rodríguez Fernández, Meredith Whittaker, Benjamin Pyle, James Farrar, Cansu Safak, Anton Ekker, Sameer Ashar, Jack Lerner, Aziza Ahmed, Stacey Dogan, James Brandt, Zohra Ahmed, Salome Viljoen, Eletra Bietti, Amy Kapczynski, Sanjay Jolly, Yochai Benkler, Tyler Sandness, Katherine Neumann, Brishen Rogers, Edward Ongweso, Kathleen Thelen, Hiba Hafiz, Pauline Kim, Sarah Myers West, David Seligman, and Terri Gerstein. The author also thanks the organizers and attendees of the following conferences where this Essay was workshopped: the 2024 Harvard Law and Political Economy Technology Workshop, the 2024 MIT-Boston College American Political Economy Workshop, and the II Seminário Nacional do Movimento Advocacia Trabalhista Independente do Brasil. Additionally, I thank the Omidyar Network—and in particular Thea Anderson, Director for Digital Identity, and Amal Chaddha, Principal—for their generous support in funding the research that informs this Essay. Finally, I am deeply grateful to the editors of the Yale Law Journal, *Yang Shao, Paige E. Underwood, Lily Moore-Eissenberg, Beatrice L. Brown, and Deja R. Morehead, for their patience, brilliant feedback, and excellent editing skills.*