Data Subject Rights as a Tool for Platform Worker Resistance

Lessons from the Uber/Ola Judgments

Li, W.; Toh, J.

DOI
10.31219/osf.io/cxhv4
10.5040/9781509965939.ch-006

Publication date
2023

Document Version
Author accepted manuscript

Published in
Data Protection and Privacy

Data Subject Rights as a Tool for Platform Worker Resistance: Lessons from the *Uber/Ola* Judgments

Wenlong Li* and Jill Toh*

This chapter will appear in the CPDP 2022 Conference Book to be published with Hart. If needed, please refer to the final version.

Abstract

Data subject rights have been increasingly used to challenge power asymmetries in different contexts, including work. This chapter looks at how platform workers have harnessed their data subject rights in the General Data Protection Regulation (GDPR) in the wider context of platform worker resistance. The strategic litigation cases against Uber and Ola, brought forth by App Drivers Workers Union (ADCU) and Worker Info Exchange (WIE) before the Amsterdam District Court (ADC), represent a prime example of data subject rights being leveraged by workers in an unconventional and potentially complicated manner. While this is not the first time that data subject rights have been interpreted before courts, these judgments have implications that merit attention from both labour protection and data protection communities. These rulings showcase how data rights are operationalised and envisioned as a tool of resistance, contrasting with how these rights are designed by legislators. These rulings also reveal barriers to the effective exercise of these rights in practice, which should be urgently addressed via an update on the guidelines or via more radical reform. This chapter evaluates the ADC's rulings through the lens of data protection and shows glitches, mismatches and erroneous views in need of revision in the appeal. It is argued that courts are in a distinctive and

* University of Birmingham, UK.

* University of Amsterdam, The Netherlands.

The authors would like to thank the organisers and participants of the Digital Ideas Lunch Series 'Law in an Algorithmic Society' 2021, Digital Legal Talks 2022 and CPDP 2022 for providing us with a platform to test our ideas, and for all the comments and input on our earlier iterations. In particular, we are very grateful to Niklas Eder, Silvia de Conca, Jef Ausloos and Joris van Hoboken for their time and extensive feedback. We are also thankful and deeply inspired by the conversations with James Farrar, Yaseen Aslam and Anton Ekker, who are fundamental to writing this chapter. This work was made possible by the Digital Transformation and Decision-Making initiative at the University of Amsterdam, as part of the Law Sector Plan in the Netherlands.

critical position vis-a-vis data protection authorities to make these rights work. While there are inherent limitations on these rights (the right of access in particular), courts play an indispensable role in removing procedural barriers and establishing avenues for balancing competing values. At the juncture where the regulatory landscape for platform work are being radically re-configured, data subject rights still, we argue, offer potentials for platform workers as a tool of resistance.

Keywords

GDPR, data rights, right of access, right to data portability, right not to be subject to automated decision-making, right to explanation, Uber/Ola, platform worker, resistance

I. Introduction

The emergence of the platform economy has brought about many changes for workers. The assumed benefits associated with platform work include flexibility, autonomy and the ability to decide their own working rhythm. Yet, the reality of platform workers shows otherwise. Through a combination of legal, technical and political strategies, platforms have consistently argued that platform workers are independent contractors. One key component of their strategy has been to delegate and outsource managerial functions via algorithmic systems, otherwise known as algorithmic management. [1] The platforms seek to absolve their responsibilities via opaque algorithmic systems, creating an illusion that 'your boss is an algorithm'. [2] These developments have intensified the challenges platform workers face, including pervasive surveillance and control, a lack of transparency and understanding of their working conditions, discrimination and increasing precarity, amongst other struggles.

[1] Jeremias Adams-Prassl, 'What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work,' *Comparative Labor Law and Policy Journal* 41.1 (2019): 131.

[2] Antonio Aloisi and Valerio de Stefano, *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour* (London: Bloomsbury Publishing, 2022), 7.

Despite many odds stacked against platform workers, they have responded to their unjust situation with new tactics and strategies.[3] As many commentators point out, (big) data has become a new frontier in the battle for workers' rights, given the intensified level of surveillance, constant monitoring, and the precarity of workers exacerbated by algorithmic management.[4] Indeed, in parallel with the litigation cases concerning better employment protections, platform workers are now actively leveraging their data subject rights provided by the General Data Protection Regulation (GDPR). These rights, characterised in the public debate as a tool of resistance,[5] do complement the workers' existing fight for a more sustainable and safe platform economy and create new forms of data-enabled opportunities.[6]

There are instances in case-law[7] or administrative measures[8] in which work-related needs are considered in the context of privacy and data protection. With a focus on the processing of personal data, however, little is said about algorithmic management. The only exception seen is the Italian DPA's imposition of fines on Foodinho (subsidiary of Glovo), a food delivery company, for having no safeguards in ensuring fairness and accuracy in the algorithms used to rate riders' performance, and for insufficient procedures to contest algorithmic decisions with a human decision-maker.[9] The four judgments delivered by the ADC in March 2021 vis-à-vis ride-hailing platforms Uber and Ola represent a timely and invaluable addition to this understated problem in the context of data protection.

---

[3] Ioulia Bessa, Simon Joyce, Denis Neumann, Mark Stuart, Vera Trappmann, and Charles Umney, *A Global Analysis of Worker Protest in Digital Labour Platforms* (Geneva: International Labour Organiation, 2022).

[4] Laurie Clarke, 'Data is the Next Frontier in the Fight for Gig Workers' Rights,' *Tech Monitor*, techmonitor.ai/policy/education-and-employment/data-next-frontier-fight-for-gig-workers-rights.

[5] Karen Gregory, '"Worker Data Science" Can Teach Us How to Fix the Gig Economy,' *WIRED*, www.wired.com/story/labor-organizing-unions-worker-algorithms/.

[6] Gregory (n. 5).

[7] *Lopez Ribalda and Others v Spain* [GC] no. 1874/13. *Barbulescu v Romania* [GC] no. 61496/08. *FILCAMS CGIL, NIDIL CGIL, FILT CGIL v. Deliveroo Italia S.R.L.* no. 2949/2019.

[8] EDPB, 'Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre,' *EDPB*, edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en. EDPB, 'The Icelandic DPA has fined a company running ice cream parlours for processing employee's personal data via video surveillance camera installed in an employee area,' *EDPB*, edpb.europa.eu/news/national-news/2021/icelandic-dpa-has-fined-company-running-ice-cream-parlours-processing_en.

[9] EDPB, 'Riders: Italian SA Says No to Algorithms Causing Discrimination: A platform in the Glovo group fined EUR 2.6 million,' *EDPB*, edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en.

This chapter evaluates the four judgements through the lens of data protection. While it is not the first-time data subject rights are considered before courts, these rulings engage a previously understated but practically important situation. While the several GDPR rights are designed to be separate in pursuit of distinct purposes, these rights are often used jointly in practice to achieve an objective not necessarily aligned with one or more purposes articulated for these rights. From the perspective of platform workers, for instance, checking the accuracy of personal data collected or lawfulness of data processing conducted is of little practical use. Data subject rights are often imagined instead as a tool to address power and information asymmetries and ultimately to address their work-related needs. The four Dutch cases vividly present the collective thinking of platform workers to pool individual datasets with a view to building a union-backed data trust. While the idea stands sound and reasonable, it runs counter to how data subject rights are perceived, expected and interpreted. It is on the basis of this tension that this chapter proceeds.

The chapter is organised as follows. After this introduction, section II contextualises the workers' exercise of their data subject rights within the platform worker resistance literature. Section III presents the details of the four Dutch judgments in a systematic and structured manner while paving the way for further analysis. Sections IV and V attend respectively to the micro and macro perspectives of data subject rights. We analyse in section IV a set of challenges that hinders the effective exercise of three data subject rights revealed by the judgments. Section V engages with broader concerns about data subject rights as a tool of resistance.. These perspectives are then connected in Section VI with the ongoing legislative developments in the EU, including the proposed EU Directive on improving working conditions in platform work (hereinafter the 'proposed Platform Work Directive') and the proposed Artificial Intelligence (AI) Act. Section VII concludes.

II. Platform Work: Challenges and New Forms of Resistance

Platform economy is an umbrella term[10] that encompasses types of labour mediated by digital platforms. It extends across a spectrum of unpaid, micropaid and poorly paid human tasks[11] and has been part of a larger shift in work and employment, altering the ways in which work is managed and re-organised.[12] This chapter focuses on on-demand platforms, a sub-set of the platform economy that involves platform work geographically tethered and location-based (specifically in Europe) by allocating service-oriented tasks through location-based apps. Ride-hailing and courier delivery services such as Uber, Deliveroo, Bolt are prime examples of this type of platform.[13] Platform workers in this sector have been actively campaigning, organising, resisting and demanding better pay and working conditions, but also reimagining the ways in which data and technology can be utilised in service of workers, not capital.[14]

A. The Platform Economy and its Challenges for Workers

The emergence of platform companies was initially touted as innovative and disruptive. Yet, developments in the platform economy over the past five years have proven to be otherwise. The platform economy can largely be characterised as a continuation of long-existing trends of the casualisation of work, whereby employment protections are eroded and replaced by zero-hour contracts and workers take on the risk of the contract. [15] What is novel is its intersection with technological developments, such as algorithmic management, which exacerbates the

[10] Identifying proper terminology has been a major challenge that underlies the work and commentary in these areas and many scholars, researchers and policymakers do not explicitly agree on a definition. See Orly Lobel, 'The Law of the Platform,' *Minnesota Law Review* 137 (2016): 88. Deepa Das Acevedo, 'Regulating Employment Relationships in the Sharing Economy,' *Employee Rights and Employment Policy Journal* 20 (2016): 3.

[11] Tiziana Terranova, 'Free Labor: Producing Culture for the Digital Economy,' *Social Text* 18.2 (2000): 34. Trebor Scholz, 'Introduction: Why does Digital Labor Matter Now?,' in *Digital Labor: The Internet as a Playground and Factory*, ed. Trebor Scholz (New York: Routledge, 2012), 1.

[12] Brishen Rogers, 'The Law and Political Economy of Workplace Technological Change,' Harvard Civil Rights-Civil Liberties Law Review 55.2 (2020): 539. Antonio A. Casilli, 'Digital Labor Studies Go Global: Toward a Digital Decolonial Turn,' *International Journal of Communication* 11 (2017): 3934–3935.

[13] Jamie Woodcock and Mark Graham, *The Gig Economy: A Critical Introduction* (Cambridge: Polity Press, 2020), 55.

[14] Gregory (n. 5).

[15] Adams-Prassl (n. 1) 133.

already precarious position of workers.[16] Businesses have long used technology to build hierarchal relations with workers, including surveillance and monitoring, and the pervasiveness of modern technologies are *qualitatively* different and significant.[17] Some scholarship has documented the contractual dimension of platform work, such as the (mis)classification of employment through independent contractor statuses (or 'bogus self-employment') through narratives of flexibility and autonomy, which has impacted workers' access to basic labour rights and protections.[18] These basic employment protections provide rights to minimum wage, social protection, freedom of assembly, protection from unfair dismissals and discrimination. Other scholarship focuses on the ways in which algorithmic management re-organises labour processes and alters managerial prerogatives,[19] with implications for platform workers' income, job security, autonomy and control at work.[20] For workers, algorithmic management includes forms of granular managerial control via systems that range from gamification strategies to GPS tracking, to task allocation, to price-setting, to ratings and to deactivation (or 'robo-firing'). Due to the mediation of work through opaque algorithmic management systems, workers are unable to understand how their wages are calculated, how performance metrics are weighted, or how they are discriminated against. Further instances of opacity include why workers are unable to login to their app and why they have been deactivated. Platform companies rely on information asymmetries and control mechanisms to

---

[16] Mohammad Amir Anwar and Mark Graham, 'Between A Rock and A Hard Place: Freedom, Flexibility, Precarity and Vulnerability in the Gig Economy in Africa,' *Competition & Change* 25.2 (2020): 249.

[17] Phoebe Moore, Martin Upchurch and Xanthe Whittaker, 'Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism,' in *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, eds. Phoebe Moore, Martin Upchurch and Xanthe Whittaker (Cham: Palgrave Macmillan, 2018), 3–4. Valerio de Stefano, '"Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work,' *International Journal of Comparative Labour Law and Industrial Relations* 36.4 (2020): 427.

[18] Valerio de Stefano, 'The Rise of the "Just-in-Time Workforce": On-Demand Work, Crowdwork, and Labor Protection in the "Gig-Economy",' *Comparative Labor Law and Policy Journal* 37.3 (2016): 495. Veena B. Dubal, 'Winning the Battle, Losing the War?: Assessing the Impact of Misclassification Litigation on Workers in the Gig Economy,' *Wisconsin Law Review* 4 (2017): 792.

[19] Aloisi and de Stefano (n. 2) 28. Adams-Prassl (n. 1) 131.

[20] Melissa R. Cano, Ricard Espelt and Mayo Fuster Morell, 'Flexibility and Freedom for Whom? Precarity, Freedom and Flexibility in On-demand Food Delivery,' *Work Organisation, Labour & Globalisation* 15.1 (2021): 49–52.

manage, constrain and coerce workers.[21] These forms of control differ from traditional ones as they allow for decreased accountability via the 'outsourcing' of managerial functions to algorithmic systems.[22] Platform companies also shift a variety of risks onto workers, whether they be financial, mental, physical, occupational health, or safety risks. [23] Additionally, different forms of discrimination related to price, wage, or race have also been widely reported.[24]

While there are varied experiences amongst platform workers, the structural effects of these ongoing developments intensify the precarity and exploitation of platform workers, whose full-time workforce often belongs to racialised, marginalised, migrant communities.[25] At the core, platform workers lack legal protection on two fronts: employment protection and redress mechanisms related to transparency in algorithmic and automated decision-making systems.

B. Platform Worker Resistance: New Tactics and Strategies

The atomised nature of on-demand platform work has posed significant challenges to collective organising. Still, platform workers have been actively campaigning for better working conditions, protection, pay and notably, insight into platform data and algorithmic systems.[26] In reaction to the changing labour context, platform worker resistance encompasses new tools and strategies to subvert, resist and challenge the current situation in the platform economy. Some authors have rightly cautioned against such optimism by questioning how these efforts can be sustained, particularly as platform companies find ways to structurally break the power

---

[21] Lutfun Nahar Lata, Jasmine Burdon and Tim Reddel, 'New Tech, Old Exploitation: Gig Economy, Algorithmic Control and Migrant Labour,' *Sociology Compass* (2022): 3–4.

[22] Alessandro Gandini, 'Labour Process Theory and he Gig Economy,' *Human Relations* 72.6 (2018): 1046. Lata, Burdon and Reddel (n. 21) 5.

[23] Karen Gregory, "'My Life is More Valuable Than This": Understanding Risk among On-Demand Food Couriers in Edinburgh,' *Work, Employment and Society* 35.2 (2020): 323–328.

[24] Akshat Pandey and Aylin Caliskan, 'Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms,' *AIES 2021 – Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (2021): 827. Veena Dubal, 'The New Racial Wage Code,' *Harvard Law and Policy Review* 15.2 (2021): 526.

[25] Moritz Altenried, 'Mobile Workers, Contingent Labour: Migration, the Gig Economy and the Multiplication of Labour,' *Environment and Planning A: Economy and Space* (2021): 6.

[26] Gregory (n. 5).

of organised labour.[27] However, these efforts by platform workers persist, and new forms of resistance, protests and contestation are emerging in the platform economy. Overall, platform worker resistance is a combination of legal and non-legal strategies, including on-the-ground and online activities, which can be categorised as the following:

(a) **Online and offline coordination:** Workers coordinate demonstrations, strikes and boycotts, through formal channels such as unions, but also increasingly through informal ad-hoc worker collectives and co-operatives.[28] This involves riders organising themselves and coordinating strike action with other service sector workers, through encrypted chats and informal groups online and offline.[29]

(b) **Algorithmic activism:** Workers build and develop software or apps to 'game the system' and counteract changes in their app environment by manipulating or gaining an advantage over the platforms they work for.[30] It can also range from simple acts such as drivers resisting and rejecting performance metrics by cancelling rides,[31] to more sophisticated methods of using software to identify the location of a passenger's destination and simultaneously identifying more expensive journeys before deciding to accept a ride.[32] Increasingly, workers together with programmers, researchers, unions and activists are attempting to create data-enabled opportunities for the benefit of workers. They are building coalitions and pooling resources to build tools and apps to offer more insight into how algorithmic systems calculate wages, track working time and identify wage theft.[33] This has increasingly expanded to developing new (formalised and less formalised) ways of collectivising around data, including data trusts and data co-ops, in order to collectivise and port data, as evident in the cases below.[34] These forms

---

[27] Niels van Doorn, 'At what Price? Labour Politics and Calculative Power Struggles in On-demand Food Delivery,' *Work Organisation, Labour & Globalisation* 14.1 (2020): 146–147. Niels van Doorn and Julie Yujie Chen, 'Odds Stacked against Workers: Datafied Gamification on Chinese and American Food Delivery Platforms,' *Socio-Economic Review* 19.4 (2021): 1362.

[28] Bessa et al. (n. 3) 10. Hannah Johnston and Chris Land-Kazlauskas, *Organizing On-Demand: Representation, Voice, and Collective Bargaining in the Gig Economy* (Geneva: International Labour Organisation Conditions of Work and Employment Series, no. 94) (2019): 5, 18.

[29] Callum Cant and Jamie Woodcock, 'Fast Food Shutdown: From Disorganisation to Action in the Service Sector,' *Capital & Class* 44.4 (2020): 516. Callum Cant, *Riding for Deliveroo: Resistance in the New Economy* (Cambridge: Polity, 2020), 94.

[30] Julie Yujie Chen, 'Thrown under the Bus and Outrunning It! The Logic of Didi and Taxi Drivers' Labour and Activism in the on-Demand Economy,' *New Media & Society* 20.8 (2018): 2691.

[31] Mareike Möhlmann and Lior Zalmanson, 'Hands on the Wheel: Navigating Algorithmic Management and Uber Drivers' Autonomy,' *Proceedings of the International Conference on Information Systems (ICIS) Seoul, South Korea (December 2017):* 3.

[32] *ADCU v Uber* B.V. C/13/692003/HA RK 20-302.

[33] Gregory (n. 5).

[34] 'About WIE,' Worker Info Exchange, www.workerinfoexchange.org/. 'About GigCV,' Gig CV, gigcv.org/. Ada Lovelace Institute, Exploring legal mechanisms for data stewardship (London: Ada Lovelace Institute, 2021), www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.

of resistance build on earlier initiatives such as worker resistance in clickwork.[35] While there remains ethical, technical and practical concerns beyond the scope of this chapter, some of these efforts have supported platform workers in gaining transparency and insight into their working conditions.

(c) **Deploying data subject rights (and other laws) to counter power asymmetries, including strategic litigation:** Workers are bringing forth legal action such as (strategic) litigation, despite challenges to accessing institutional channels of worker contestation, and the costs and resources associated with litigation. One legal tool which has emerged to challenge information and power asymmetries is data subject rights under the GDPR. In parallel with other litigation cases brought forward by platform workers related to employment status,[36] minimum wage[37] and discrimination,[38] platform workers in Europe are also asserting their data subject rights[39] to complement their existing struggles for stronger legal protection. This 'interlegality'[40] may offer different opportunities to define legal entry points for litigation, and to think more thoroughly how asserting data subject rights and strategic litigation can fit into the wider strategy of platform worker resistance.[41]

The legal ambiguity surrounding platform workers' status as independent contractors means that they are unable to claim basic worker rights associated with employment law. However, data subject rights' purpose-blind and intent agnostic nature offers some potential for platform workers in Europe to gain transparency into algorithmic systems and processes that mediate and shape their work, including understanding how their labour generates value for platform

---

[35] Lilly C. Irani and Michael Six Silberman, 'Turkopticon: Interrupting Worker Invisibility in Amazon Mechanical Turk,' *CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (April 2013): 611.

[36] Valerio de Stefano and Antonio Aloisi, 'European Legal Framework for "Digital Labour Platforms",' *Publications Office of the European Union* (2018): 41.

[37] Ruth Berins Collier, Veena B. Dubal, and Christopher L. Carter, 'Disrupting Regulation, Regulating Disruption: The Politics of Uber in the United States,' *Perspectives on Politics* 16.4 (2018): 921.

[38] Chris Vallance, 'Legal action over alleged Uber facial verification bias' (*BBC*, 8 October 2021), www.bbc.com/news/technology-58831373.

[39] Hießl, Christina, 'Case law on Algorithmic Management at the Workplace: Cross-European Comparative Analysis and Tentative Conclusions,' *European Commission, Directorate DG Employment, Social Affairs and Inclusion* (September 2021): 4. papers.ssrn.com/sol3/papers.cfm?abstract_id=3982735. Cansu Safak and James Farrar, *Managed by Bots: Data-Driven Exploitation in the Gig Economy* (London: *Worker Info Exchange*, 2021), www.workerinfoexchange.org/wie-report-managed-by-bots.

[40] Interlegality is defined by de Sousa Santos as 'a highly dynamic process because the different legal spaces are non-synchronic and thus result in uneven and unstable mixings of legal codes'. See Boaventura de Sousa Santos, 'Law: A Map of Misreading. Toward a Postmodern Conception of Law,' *Journal of Law and Society* 14.3 (1987): 298.

[41] Yaseen Aslam and Jamie Woodcock, 'A History of Uber Organizing in the UK,' *South Atlantic Quarterly* 119. 2 (2020): 415. Bessa et al. (n. 3) 7, 8.

companies.[42] These rights can be invoked by any individual whose fundamental rights, freedoms or interests have been affected by the processing of personal data and automated decision-making,[43] which can overcome some of the existing complications of employment status and its associated rights. For instance, in some cases, data subject rights can act as a mechanism and first step to prove and address other forms of harms. As documented in the Managed by Bots report,[44] Uber driver Pa Edrissa Manjang was deactivated by Uber for failing his selfie identity verification via facial recognition software, which has been proven to have a high rate of inaccuracy on darker skinned people.[45] Pa, together with ADCU, submitted a subject access request in order to obtain the selfies he had submitted to prove that he was wrongly dismissed, as well as to bring forth a case against Uber to challenge the use of its racially discriminatory facial recognition system.

While there have been criticisms that data subject rights are individualistic in nature, a growing body of work seeks to emphasise the potential of data subject rights in protecting collective interests.[46] The sentiment of harnessing the collective potential of data subject rights is also echoed by advocates of worker and data subject rights, stressing the importance for unions (and workers) to seriously reckon with the impact that algorithmic management, and other technologies, have on workers. Their call is for unions to build capacity and resources to inform workers about their data subject rights, support their process in asserting rights, as well as to negotiate for better collective (worker) protections in upcoming data and technology legislative proposals.[47] Furthermore, researchers working on digital labour have demonstrated the lack of

---

[42] Gregory (n. 5).

[43] Jef Ausloos, René Mahieu and Michael Veale, 'Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance,' *Journal of Intellectual Property, Information Technology and E-Commerce Law* 10.1 (2019): 283.

[44] Safak and Farrar (n. 39) 17–21.

[45] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,' *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81 (2018): 77.

[46] René Mahieu, Hadi Asghari, and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect,' *Internet Policy Review* 7.3 (2018): 15–17. Joanna Mazur, 'Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law,' *Erasmus Law Review* 11 (2018): 183. René Mahieu, and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards An Ecology of Transparency,' *Internet Policy Review* (2020).

[47] Christina Colclough, 'Towards Workers' Data Collectives,' *IT for Change*, projects.itforchange.net/digital-new-deal/2020/10/22/towards-workers-data-collectives/. Nakeema Stefflbauer, 'When Human rights + Digital

labour perspectives and consideration of labour rights within legal discussions surrounding data and technology regulation, despite the significant implications technology will continue to have on work.[48]

The collective dimension is beginning to be addressed by other EU legal developments in reaction to algorithmic management and the datafication of the workplace, such as the proposed Platform Work Directive and the proposed AI Act. These developments may bring about some clarity for the GDPR, but also more complexities as the GDPR interacts with other legal instruments. As such, the relevance in assessing the cases brought forward by Uber and Ola drivers at the ADC has particular importance from both a data protection and labour perspective.

III. The *Uber/Ola* Judgments: An Overview

A. Context

In order to contextualise these cases, it is first important to understand why Uber and Ola drivers brought forward these cases against Uber and Ola. First, they wanted to prove an employment relationship by understanding the extent to which Uber and Ola exerted management control by means of algorithmic systems and automated decision-making. These cases were brought forward against the background of the six year-long employment reclassification case at the UK Supreme Court, where the court was assessing the degree in which these companies exert management control by means of algorithmic and automated decision-making systems.[49] Second, they wanted to calculate minimum wage and holiday allowances. Third, they wanted protection from discrimination, and the drivers' ratings can be

---

rights = Workers' rights,' *Digital Freedom Fund*, digitalfreedomfund.org/when-human-rights-digital-rights-workers-rights/.

[48] Lina Dencik, 'Towards Data Justice Unionism? A Labour Perspective on AI Governance,' in *AI for Everyone: Critical Perspectives*, ed. Pieter Verdegem (Westminster: University of Westminster Press, 2021), 286. Niklas Jędrzej, and Lina Dencik, 'What Rights Matter? Examining the Place of Social Rights in the EU's Artificial Intelligence Policy Debate,' *Internet Policy Review* 10.3 (2021): 20–23.

[49] These cases were brought forward between July 2020 and December 2020, where the employment reclassification case at the UKSC was still ongoing. The ruling by the Supreme Court was passed down in February 2021. See also, Jill Toh, 'UK gig drivers recognised as workers – what next?,' (*Social Europe*, 25 February 2021), socialeurope.eu/uk-gig-drivers-recognised-as-workers-what-next.

severely affected if customers discriminate against them. Falling below an average rating of 4.4 (for reasons that are not wholly transparent) for drivers means that they are deactivated and 'fired'. Fourth, they wanted their data in order to understand the rationale of these systems for collective bargaining and advocacy. Lastly, they wanted to establish a data trust to be managed by Worker Info Exchange.

For these reasons, this chapter underscores the significance of these cases when considered from a broader perspective. These cases move beyond the idea that platform workers simply want to understand their minimum wage and working conditions. Rather, these drivers have longer-term goals in mind. They seek to harness their data subject rights with plans to intervene in other areas such as employment and discrimination law. Furthermore, the drivers' goal of establishing a data trust for their grassroots union demonstrates a forward-thinking initiative to rethink how information about one's data can be collectivised to the benefit of workers. In effect, these strategic litigation cases are situated within their wider strategy to fight and advocate for better workers' rights and protection, as well as to reimagine new forms of organisation.

B. Rulings

A total of four judgments were delivered by ADC on 11 March 2021, all of which are concerned with platform drivers strategically exercising GDPR data subject rights vis-à-vis ride-hailing platforms. The plaintiffs of these cases are mostly drivers based in the UK, the Netherlands and Portugal, supported by the ADCU.

In *Uber Access*,[50] ten UK-based drivers and one from Portugal filed a complaint against Uber in Amsterdam, where its European headquarter sits. Described by the media as a victory of Uber to 'fend off wide-ranging requests for data from drivers',[51] the results of this judgment were actually mixed. Indeed, the majority of access requests per Article 15 GDPR were rejected, involving the access to manual notes, 'tags', internal 'reports', to name a few. The reasons for

[50] *Uber Access*, C/13/687315/HA RK 20-207.

[51] Natasha Lomas, 'Dutch Court Rejects Uber Drivers' "Robo-Firing" Charge but Tells Ola to Explain Algo-Deductions,' *TechCrunch*, techcrunch.com/2021/03/12/dutch-court-rejects-uber-drivers-robo-firing-charge-but-tells-ola-to-explain-algo-deductions/.

rejection are diverse, including that the drivers' requests were not specific enough, that data access may adversely affect the rights and freedoms of others (e.g., Uber customers). The court dismissed data portability requests under Article 20 on the basis that the data had already been provided to the Uber drivers in PDF format, which were deemed to be adequate and GDPR-compliant. When it came to ratings, ostensibly one of the most valuable datasets for workers to continue their work on a platform or to switch to another, the court was on the side of drivers. It was held that ratings should be provided to the drivers but in an *anonymised* form for the protection of third-party privacy.

In *Ola Access*,[52] three UK-based drivers sued the Bangalore-based ride-hailing platform Ola. Previously, Ola responded by providing a collection of documents and files, which the drivers found neither adequate nor consistent. For instance, many categories of data described in Ola's Privacy Statement or Guidance Notes were either missing or not in a requested format (ie, CSV). Moreover, the explanation for Ola's use of automated decision-making was deemed not meaningful, hence prompting the drivers to demand full access to their data. Notably, the drivers detailed the types of data and information sought as well as the legal basis on which such access is requested.[53] Three main breakthroughs are made in this case. First, the court upheld in a similar fashion a request to access ratings but only in an anonymised form. Second, it supported for the first time requests to improve the transparency of various profiles established by Ola, notably including the fraud probability score, the earning profile and the Guardian system built to 'detect irregularities'.[54] It was held that the drivers are entitled, under Article 15, to access to the personal data 'used to draw up the risk profiles as well as information about the segments into which the applicants have been classified'.[55] Note that this profile transparency achieved was not on the basis of Article 22 but Article 15, because the explanation requests (on the basis of Article 22) were not admitted due to the burden of proof imposed on the drivers. Third, when it came to data portability, the court declared irrelevant the purpose for which such data are requested on the basis of Article 20 GDPR. In other words, the Ola

[52] *Ola Access*, C/13/689705/HA RK 20-258.

[53] ibid 3.1.

[54] ibid 4.48.

[55] ibid 4.36, 4.45.

drivers do not have to show 'any particular interest or state the goal that [they] want to achieve with the access'.[56] Additionally, the court dismissed all the requests on the basis of Article 22 for not meeting the legal requirements such that the decision has to be made 'solely based on automated decision' or that the decision produces a legal or similarly significant effect.

The remaining two judgments are related to 'robo-firing' and concerned with Article 22 rights vis-à-vis Uber. In *Uber Deactivation I*,[57] three UK-based drivers and one from Portugal received a notification from Uber about the deactivation of their driver accounts. These drivers were punished for allegedly committing fraud and thereby violating Uber's Terms of Conditions. Related to the previous cases supported by the ADCU, the drivers' main request was not re-activation but the provision of meaningful information about the algorithmic decisions made. Again, the court delivered mixed results. On the one hand, the requests of two drivers were rejected as they had previously been given an explanation within Uber's messaging system which was deemed by the court to be sufficiently clear (without an explicit content analysis). On the other hand, two other drivers succeeded in their request for an explanation as they had not been provided with any information about why their accounts had been deactivated.

Lastly, *Uber Deactivation II* concerns five UK-based drivers and one from the Netherlands who complained that they had been wrongly accused of fraudulent activities and, as a result, dismissed by the algorithms deployed by Uber. The court held in favour of the drivers that their accounts be reinstated simply because Uber was absent during the proceedings.

It is also worth noting that drivers requested compensation and punitive measures in all the cases, but most claims were rejected as the court did not see 'reasons for damage to their humanity or good name or damage to their person in any other way'.[58] The only exception is *Uber Deactivation II*, in which the court upheld the compensation requested by the drivers, as well as an imposition of penalty for non-compliance, largely due to Uber's absence in the proceedings.

---

[56] ibid 4.6.

[57] *Uber Deactivation I*, C/13/692003/HA RK 20-302.

[58] ibid 4.31.

Case Title	Case Reference	Plaintiffs	Request	Outcome	Penalty
Uber Access	C/13/687315 / HA RK 20-207	10 UK-based & 1 Portuguese drivers	Data access via Arts 15, 20, and 22 rights in a commonly used, structured and machine-readable format or by means of API	All requests rejected excepts ratings (to be provided in an anonymised form)	No
Ola Access	C/13/689705 / HA RK 20-258	3 UK-based drivers	Same as above	The requests upheld include ratings (4.25) and profile transparency (4.52), including the risk probability score (4.45), earning profile (4.47), the Guardian system (4.49)	No
Uber Deactivation I	C/13/692003 / HA RK 20-302	3 UK-based & 1 Portuguese drivers	Explanation for why the accounts were deactivated and what personal data were involved for reaching that decision	The requests of two informed drivers rejected, and those of two uninformed drivers upheld	No
Uber Deactivation II	C/13/696010 / HA ZA 21-81	5 UK-based & 1 Dutch drivers	Account reinstation	Upheld	Yes (a sum of € 100,474 in damages and a penalty of € for non-compliance)

Table 1 An Overview of the Four Dutch judgments vis-à-vis Uber and Ola

IV. Micro-Perspectives: Making Data Subject Rights Work for Workers

In either case law or legal scholarship, each data subject right is considered in isolation and at a micro-level, often without attending to their structural and instrumental role within the larger data subject rights system. This complex web of rights, however, often causes confusion for regular data subjects who lack expertise of data protection and have little knowledge of the specific intention, scope, condition, exceptions of each right and the differences between them. Despite the original intentions, this chapter asks whether seamless, unhindered access to data can be achieved by a joint exercise of all data access rights, including the right of access, to data portability, and not to be subject to automated decision-making. The answer is far from

straightforward as these rights are not designed to initiate data flows, and considerable differences are seen in these rights in terms of the scope, format and nature of personal data covered. A thorough consideration of each right is thus necessary, with particular reference to their structural and instrumental roles within the subject rights system,

A. Right of Access

As a cornerstone of EU data protection law,[59] the right of access is intended to correct the information asymmetries between the data subject and the data controller. It hence serves an instrumental role in enabling further actions by the data subject (including the use of other data protection rights), what Ausloos et al. call the 'knock-on effect'.[60] In practice, the right of access is often relied upon to assist litigation cases by offering information that is otherwise inaccessible, but the legality of this use remains moot.

Established in the latter half of the twentieth century,[61] this right was originally devised to improve human readability, thus requiring personal data to be provided in a 'intelligible form'.[62] There should be a critical point of differentiation, as will be discussed later, between this right and the new right to data portability. The latter is characterised by the specific requirement of structured and machine-readable data, thus allowing for sharing and reuse.

For the purpose of initiating data flows towards workers, the right of access is advantageous in terms of the wide scope of data covered (theoretically concerning all the personal data undergoing processing) and the explicit requirement for the controller to explain the logic, significance and consequences of the algorithms deployed. In this context, access might be interpreted as viewing the information via a specific medium, e.g., on screen or via an app in contrast to obtaining a copy of data. This is contested, however, as the GDPR adds a new element to the right of access that explicitly allows the data subject to obtain a *copy* of personal data.

---

[59] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 181.

[60] Ausloos, Mahieu and Veale (n. 43) 283.

[61] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York: Cornell University Press, 1992), 263.

[62] Data Protection Directive 1995 Art 12(a). See also GDPR Art 7(2) and Recital 42.

This section considers three main controversies around the enforcement of this right examined in the *Uber/Ola* judgments: (1) the accessibility of subjective data (eg, human judgements, internal notes and legal analysis), (2) the meaning of access, and (3) the practicality of full access request.

i Subjective Data Accessibility

An outstanding issue in relation to Article 15 concerns whether subjective data – that is, opinions rather than facts – are accessible or not via Article 15 GDPR. There is ample illustration of this type of data in the *Uber/Ola* judgments, including the drivers' profile (consisting internal notes by Uber employees), 'tags' (labels in the customer service system that are used to assess the drivers' behaviour), reports of the drivers' performance, as well as the so-called 'fraud probability score' which is automatically generated. Access to these data is of critical significance to evaluate the adverse decisions made against the drivers. It begs the question whether human judgements, internal notes and legal analysis constitute personal data and hence are accessible via Article 15 GDPR. According to *YS and Others*,[63] a CJEU ruling concerning a person exercising the right of access to contest the decision of the Dutch authority about his immigration status, legal analysis may contain some personal data, but is not accessible via Article 15 because it cannot be checked for accuracy and corrected where necessary. Originating from the Netherlands, *YS and Others* has significant ramifications for the national precedents. A general rule is developed that this right does not extend to 'internal notes that contain the personal thoughts and/or opinions of employees of the controller or third parties, exclusively intended for internal consultation and deliberation'.[64] The position held by the CJEU in *YS and Others* is contestable and may have evolved over time. Given the prominence of this precedent in the Dutch jurisprudence, later developments have not been adequately considered in the *Uber/Ola* judgments. In *Nowak*, a case concerning an Irish lawyer seeking access to the exam questions and answers, an explicit divergence from *YS and Others* is observed. The CJEU held that both objective and subjective information can

[63] Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel* ECLI:EU:C:2014:2081, para 39.

[64] *Ola Access* (n. 52) 4.12. See also the three judgments from HR 29 June 2007: ECLI:NL:HR:2007: AZ4663, AZ4664 and BA3529.

constitute personal data as long as the data is, or can be linked to the data subject because of content, purpose or effect.[65]

This chapter does not purport to engage this issue of ever-expanding definition of personal data, which remains a critical point of contention in the scholarship.[66] It suffices to say that, between *YS and Others* and *Nowak*, the determination of the scope of data access is rather context-specific. A case involving access to personal data on which an immigration decision was made with a view to revealing the logic of that decision is apparently distinct from one in which access is requested to pool all the data obtainable and build a data trust. That said, divergence manifested in *Nowak* is by itself insufficient to conclude that subjective data are generally accessible via Article 15. This is because the scope of access per Article 15 should be interpreted *teleologically*, by reference to the aims of data protection law as well as the purpose for which the personal data was collected and processed.[67] Hence, while factual data are objective and verifiable, it is contested whether subjective data as such are verifiable as well (i.e., has their 'accuracy' been checked). Even if this is possible, the CJEU held in a series of case law that it is the sectoral laws (rather than data protection) that should be relied upon to contest accuracy of decisions.[68] In Wachter et al.'s words, EU data protection law grants individuals control over how their personal data are *processed*, but not how they are *evaluated*.[69] The 'accuracy' of decisions the drivers seek to check and correct was not deemed compatible with the objectives of data protection. This tradition is, however, not uncontroversial. Hallinan and Borgesius, for instance, draws on other elements of the GDPR repository, ie, the accuracy principle under Article 5 GDPR, to make a case for correcting opinions.[70] It remains to be seen how the dispute is further reflected and adapted by the court post-*Nowak*, but the teleological

---

[65] Case C-434/16, *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994, para 34.

[66] See for instance, Nadezhda Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law,' *Law, Innovation and Technology* 10.1 (2018): 40–81. Benjamin Wong, 'Delimiting the Concept of Personal Data after the GDPR,' *Legal Studies* 39.3 (2019): 517–532.

[67] *Nowak* (n. 65) para 53.

[68] See Case C-28/08 P, *European Commission v Bavarian Lager* ECLI:EU:C:2010:378. *YS* (n. 63), paras 45-46. *Nowak* (n. 65).

[69] Sandra Wachter, and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI,' *Columbia Business Law Review* 2 (2019): 443, 499.

[70] Dara Hallinan and Frederik Zuiderveen Borgesius, 'Opinions Can Be Incorrect (in Our Opinion)! On Data Protection law's Accuracy Principle,' *International Data Privacy Law* 10.1 (2020): 1–10.

tradition established by the CJEU case law might have rendered the right of access not fit for purpose.

ii The Meaning of Access

Platforms often claim that they have already provided the personal data sought. Their argument is based on the idea that drivers can view them via the apps or in their Privacy Policies. Thus, access to various types of data requested – such as the start and end of a journey, customer transactions, booking history, GPS data, device data, location data – were denied mostly on that basis. It begs the question as to: (1) whether app display constitutes a permissible form of compliance with Article 15, and (2) whether Article 15 allows for access to personal data in addition to what is presented in a Privacy Policy in accordance with Articles 13–14 GDPR.

Article 15 is almost silent on the form or means by which personal data should be provided, but the latest EDPB guidelines have provided some clarity. In brief, the EDPB does not explicitly and categorically exclude app display as a means of responding to a data access request. As such, oral information, inspection of files, onsite or remote access, and other 'non-permanent ways' of access without the possibility to download or copy data are all deemed sufficient. The EDPB only *encourages* the provision of a copy of data along with supplementary information as 'the main modality for providing access to the personal data'.[71] As significant leeway is given to the platforms to determine the meaning or means of access (as viewing rather than transmitting), and hence the scale and nature of data flows towards workers, it may therefore be concluded that Article 15 requests do not necessarily lead to *real* data flows.

Another related issue is whether the controller is obliged to provide more data or information that is presented in their Privacy Policies in the face of Article 15 requests. This relates to an unsettled issue about the relationship between Article 15 and Articles 13–14 under the GDPR. An abundance of commentaries seek to make distinctions between *ex ante* transparency and *ex post* transparency, between information for the general public (eg, provided in the Privacy Policies) and information specific about a particular processing activity concerning a data

[71] EDPB, 'Guidelines 01/2022on Data Subject Rights – Right of Access', edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en, 41-2.

subject.[72] Zanfir contends that the right of access provides 'a second, deeper and more detailed layer of information' beyond the disclosure by any Privacy Policy.[73] In her view, the key difference between Article 15 and Articles 13–14 is that the right of access allows for the obtaining of 'copies of personal data' as well as '*updated* information' compared to what is provided in the Privacy Policies. Similarly, Ausloos et al. see the added value of Article 15 as providing the 'possibility for individuals to learn more about their particular situation upon request'.[74] In reality, however, Article 15 requests have been dismissed as the court considered the Privacy Policy sufficient as a source of the requested information.[75] The guidance provided by the EDPB is not clearly disproving of this view. According to the guidelines, Article 15 request should lead to 'updated and tailored information' other than what is provided in a Privacy Policy.[76] Simply referring to the wording of a privacy policy would not be sufficient in responding to Article 15 requests.[77] Still, the guidelines indicate the circumstance to be an exception where 'tailored information is the same as the general information'.[78] The example provided by the EDPB, ie, the information about the right to complain, does imply that such a circumstance is rare.

iii The Practicality of Full Access Request

The last point of contention is whether it is practically possible to make a successful request for access to a full range of personal data undergoing processing. A full range request is not uncommon; it is encouraged as a means to maximise the potential of data subject rights.[79] In the Dutch rulings, the drivers strategically built their requests upon Articles 15, 20 and 22 while

[72] See for instance Jef Ausloos and Michael Veale, 'Researching with Data Rights,' *Technology and Regulation* (2021): 136–57. Lilian Edwards and Michael Veale. 'Slave to the Algorithm? Why A Right to Explanation Is Probably Not the Remedy You Are Looking For,' *Duke Law & Technology Review* 16.1 (2017): 18–84.

[73] Gabriela Zanfir-Fortuna, 'Right of Access by the Data Subject,' in The EU General Data Protection Regulation (GDPR): A Commentary, ed. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechesler (Oxford: Oxford University Press, 2020), 452.

[74] Ausloos, Mahieu and Veale (n. 43) 293.

[75] See, for instance, *Uber Access* (n. 50).

[76] EDPB (n. 71) 41-2.

[77] ibid.

[78] ibid.

[79] See for instance, Michael Veale, 'A Better Data Access Request Template,' michae.lv/access-template/.

demanding full access to their personal data in accordance with these provisions. This strategy, however, met with various practical hurdles.

The EDPB guidelines explicitly recognise a 'right to *full* disclosure of all data relating to them'.[80] Yet, this right is subjected to a number of exceptions, thus rendering its scope of application significantly limited. These exceptions include: (1) voluntary and explicit limitations or specifications made by the data subject, (2) reasonable doubts by the controller in the case of a large volume of data, (3) manifestly unfounded or excessive access requests, (4) requests that adversely affect the rights and freedoms of others.[81]

As is evidently shown in the Dutch judgments, a full access request is far from reality as the controller is able to cling to at least one of the exceptions stated above. Chief among them is the discretion afforded to the controller to ask for specification in cases where large volumes of data are concerned. Note that this discretion is not explicitly stated in Article 15 but merely in a non-binding recital.[82] Further, the concept of 'large volume of data' is left undefined, thus making this mechanism highly elusive. In theory, this specification requirement represents a fair balance between the data subject's right of access and the burden imposed on the controller to search, identify and provide the requested data. It can, however, be easily abused or misinterpreted in practice. For instance, a range of personal data in the *Uber/Ola* judgments, such as 'in app messages', device data and driving behaviours, are denied access on the sole ground that the drivers failed to specify their requests.[83] In *Ola Access*, the court's view about specification was even erroneously extended to the right to data portability as it found the drivers' portability request 'too general and so not specific that it must be rejected as insufficiently determined'.[84] Misinterpretations aside, it may be concluded that a full access request is rife with uncertainties. The way in which Article 15 is formulated within the GDPR makes data flows arising out of Article 15 requests inherently intermittent and partial.

---

[80] EDPB (n. 71) 35, fn 14.

[81] ibid.

[82] GDPR Recital 63.

[83] *Ola Access* (n. 52) 4.17, 4.31. *Uber Access* (n. 50) 4.35, 4.54.

[84] *Ola Access* (n. 52) 4.60.

The right of access is given a new life under the GDPR, with its scope and nature refined incrementally through court interpretation. Still, numerous factors constraining the form, purpose and scope of access would prevent the right from being a working vehicle for driving data flows. As will be argued later, even when exercised in tandem with other access rights, its advantage (eg, potentially covering all personal data concerned) cannot be fully realised.

B. The Right to Data Portability

The right to data portability is, strictly speaking, the only right newly introduced in the GDPR with no precursor in the 1995 Directive. In the early days of the GDPR's legislative process, this right was expected to be a game-changer that would fundamentally reconfigure the flow of personal data, hence exerting an impact of competition similar to number portability in the telecom sector.[85] This ambition was significantly attenuated in a later stage, with a refined objective of individual control over personal data written into the GDPR. Numerous conditions, restrictions and exceptions were added in the later phase of the GDPR's legislative process to contain its potential impact. The right is, as a result, criticised for its complexity and lack of certainty. In spite of some clarity provided by the guidelines from the Article 29 Working Party (A29WP), the predecessor of the European Data Protection Board, the applicability and effect of this right remains unclear.

Within the GDPR, the new right to data portability has a contentious status. This is partly because the right does not straightforwardly serve the purpose of data protection law, namely the protection of personal data, and partly because the right of access (strengthened by the GDPR) may arguably serve an equivalent function pursuant to Article 15(4).

By requiring the personal data to be provided in a 'commonly used, structured and machine-readable format', the right to data portability is intended to facilitate data sharing and reuse, thus making it ideal for driving personal data towards new processing systems eg, a data trust. The right's real capacity to drive data flows is, however, restricted by various factors. For instance, it allows the porting of *certain* personal data only, ie, the personal data provided by the data subject, actively or passively. According to the Article 29 Working Party Guidelines,

[85] European Commission, 'Commission Staff Working Paper GDPR Impact Assessment,' SEC/2012/0072 final, 28.

this criterion includes observed data but excludes inferred or derived ones.[86] Those not provided by data subjects, as well as non-personal data (including anonymous data) fall outside the scope of this right.

It is also a missed opportunity that the GDPR does not eventually mandate interoperability but only encourages interoperable format in a recital. A right to transmit is said to be created under Article 20(2). The name of this right can be misleading as the controller is not allowed to respond on the ground of 'technical infeasibility'.[87] This means that this right literally does not exist if the participating systems do not interoperate as a matter of fact.

In the *Ola/Uber* judgments, scant attention was paid by the court to this new right, with its novelty compared to the existing ones largely ignored. This section discusses two outstanding issues in the rulings, namely: (1) whether PDF is a GDPR-compliant format, and (2) whether there is an obligation to convert data into a machine-readable format.

i PDF as an Interoperable Format?

In *Uber/Ola Access*, the drivers made a joint exercise of all data access rights (including Article 22) in hopes that all data and information will be provided in a commonly used, structured and machine-readable format, or by way of an application programming interface (API) that allows for continuous, seamless and real-time access. This was not fully upheld by the court for the lawful reason that machine-readability is not a mandate for all data access rights.

Among the portable data, however, the drivers found that many of the data requested under Article 20 were not provided in CSV format as initially requested but actually in seven different ones (PDF, Docx, JEPG, PNG, MP3, WAV), many of which are not necessarily machine-readable.[88] The court particularly considered the PDF format, in which several types of data are provided, including 'Zendesk tickets', 'invoices', 'driver safety complaints' and 'driver documents'.

[86] Article 29 Working Party, 'Guidelines on the Right to Data Portability,' WP242, rev.01.

[87] GDPR Art 20(2).

[88] *Uber Access* (n. 50) 4.78.

The GDPR does not provide a definition of machine-readability but refers instead to the Public Sector Reuse Directive[89] in which it is defined as

> a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure

Given its technical complexity, the determination of a GDPR-compliant format goes beyond legal interpretation and hence should draw on expertise of data science. Ausloos and Veale reveal that PDF is designed for printing rather than for analysis.[90] According to Wong and Henderson, PDF files *may* be machine-readable if they contain text, but not so if tables, images and scans are included.[91] The A29WP Guidelines state that PDF is not compliant as data in such a format would not be sufficiently structured.[92] It is also recognised that the preservation of all metadata may ensure effective portability and reuse.[93] PDF should not be categorically deemed to be GDPR compliant or not; its lawfulness should be assessed contextually on a case-by-case basis. A more worrying issue, according to Ausloos and Veale, is the practice of intentionally transforming data into PDF files with a view to disadvantaging the data subject and foreclosing analysis opportunities. [94] Such a practice runs counter to the essence of Article 20 and should be explicitly blacklisted.

ii The Obligation to Data Conversion

Article 20 of the GDPR requires personal data to be provided in a structured, commonly used and machine-readable format. However, an understated fact is that not all data are internally managed and stored in a format as such. In practice, the controller may 'return' the requested data in the exact format it was initially provided by the data subject, particularly when it comes to semi-structured or unstructured data (such as video and audio files). This was upheld by the

---

[89] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, Art 2(13).

[90] Ausloos and Veale (n.72) 152.

[91] Janis Wong and Tristan Henderson, 'How Portable Is Portable? Exercising the GDPR's Right to Data Portability,' in UbiComp/ISWC 2018 – Adjunct Proceedings of the 2018 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2018 ACM International Symposium on Wearable Computers (New York: The Association for Computing Machinery, 2018), 911–920

[92] Article 29 Working Party, 'Right to Data Portability', 18.

[93] ibid.

[94] Ausloos and Veale (n. 72) 152.

ADC in *Uber Access* in which Uber provided data in the same format in which they have received them.[95] This raises the issue as to whether Article 20 creates an obligation to covert personal data if they are not held in a GDPR-compliant format. A textual reading of the GDPR might conclude that such a conversion is required. As the A29WP guidelines are silent on this issue, an update is urgently needed, taking into account the existence of non- or semi-structured data, as well as the costs of conversion especially when large volumes of data are concerned.

C. The Right not to be Subject to Automated Decision-making

The right not to be subject to automated decision-making is ostensibly the most contested right under the GDPR. It is considerably complex and loaded with conditions. For this reason, the UK Government is controversially seeking to further streamline or even scrap this right as part of its post-Brexit data protection reform.[96] Conceptually, this right is the most relevant in addressing the information asymmetries caused by algorithmic management. Similar to the ill-fated right to data portability, however, the Article 22 right ended up with numerous qualifications added during the legislative process. The complex formulation of this right forces workers to take a 'detour' by pooling personal data first so as to reverse-engineer the algorithms deployed.

As it currently stands, the Article 22 right faces significant structural problems. The title of Article 22 can be misleading too as a wide range of conditions and exceptions attenuate the 'intended' effect of this right, ie, not being subjected to automated decision-making. This right may be better viewed as *two-faceted*: on the one hand, the right not to be subject to automated decision-making is conditional upon several demanding conditions, such that the decision is made *solely* on automated decision-making, that the decision exerts a legal or similarly significant effect. Serious disputes arise from the application of these conditions, and the EDPB guidelines do not necessarily and adequately address them.[97] The complexity of this right has aroused a dispute in the data protection scholarship about whether Article 22 is a right

---

[95] *Uber Access* (n. 50) 4.81.

[96] DCMS, 'Data: A New Direction,' www.gov.uk/government/consultations/data-a-new-direction.

[97] Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-making and Profiling,' *Computer Law & Security Review* 34 (2018): 398–404.

or a prohibition per se.[98] On the other hand, in case such a right does not apply, Article 22 provides additional safeguards of more practical relevance. These safeguards include the right: (1) to obtain human intervention, (2) to express views, and (3) to contest the automated decision.[99] Other safeguards may be added by Member States by way of national legislation, according to Article 22(3).[100]

Unlike Article 15 and Article 20 rights, Article 22 is by nature not a data access right. Still, given the great difficulties in meeting the conditions for not being subject to automated decision-making, the practical value of Article 22 may lie with algorithmic transparency guaranteed jointly with Article 15(1)(h). This critical aspect has given rise to a large body of work disputing whether a 'right to explanation' (should) exist within the GDPR.[101]

In a similar vein, this section does not intend to unpack all the controversies around Article 22 but focuses on three critical issues raised in the Dutch judgments. Many of these issues happen to be the locus of the scholarship, including: (i) the level of human judgment, (ii) the nature of 'legal or similarly significant effect', and (iii) the right to explanation.

i. The Level of Human Judgment

Article 22 stipulates that the right applies only to the decision *solely* based on automated decision-making. This begs the question as to the level of human engagement that may render this condition unsatisfied. Binns and Veale reveal the complexity of decision-making that often

---

[98] Luca Tosoni, 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22 (1) of the General Data Protection Regulation,' *International Data Privacy Law* 11.2 (2021): 145–162. Isak Mendoza and Lee A. Bygrave, 'The Right Not to Be Subject to Automated Decisions based on Profiling,' in *EU Internet Law*, eds. Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou (Cham: Springer, 2017), 77–98. Lee A Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling,' *Computer Law & Security Review* 17.1 (2001): 17–24.

[99] GDPR Art 23(3).

[100] See generally Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations,' *Computer Law and Security Review* 35.5 (2019).

[101] Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-making and a 'Right to Explanation,' *AI magazine* 38.3 (2017): 50–57. Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,' *International Data Privacy Law* 7.2 (2018): 76–99. Andrew D. Selbst, and Julia Powles. 'Meaningful Information and the Right to Explanation,' *International Data Privacy Law* 7.4 (2017): 233–242. Margot E. Kaminski, 'The Right to Explanation, Explained,' *Berkeley Technology Law Review* 34 (2019): 189.

takes multiple stages and may involve both humans and machines.[102] Wachter et al. argue that a simple arrangement of human control of a certain level may be enough to make the Article 22 right utterly impracticable.[103] This is manifested in *Uber Deactivation I*, whereby the court agreed with Uber (that there was a EMEA Operational Risk team in-charge) while imposing the burden of proof on the drivers.

The A29WP in its ADM guidelines identifies a number of factors for determining the level of human judgement or oversight, including: (1) the independent and active position of the overseer (hence rubber-stamping disallowed), (2) the authority and competence to overturn automated decisions, and (3) the description in the controller's Data Protection Impact Assessment of the level of human involvement.[104] Thus, the analysis here is inherently contextual and contingent. What is troubling about *Uber Deactivation I* is that the onus is placed on the drivers, the victims of information asymmetries, in proving that the deactivation decisions were made fully automatically. As will be shown in the next section, this procedural aspect significantly determines the effective use of a data right and should be urgently addressed by the authorities.

ii. Significant Effect for Workers

The condition that the decision should exert a legal or similarly significant effect is also context-specific. In a wide range of cases involving Uber's fraud probability score, earning profile, batched matching system, as well as Ola's Guardian system, trip-matching system and upfront pricing system, Article 22 was deemed inapplicable in these rulings because the drivers failed to prove any legal or significant effect for workers. However, this does not mean that these systems or scores do not exert legal or a similarly significant effect. The linchpin of the problem lies, again, with the burden of proof imposed on the drivers. Notably, in *Uber Deactivation I*, a distinction is made between the effect of a termination and that of temporary automated blocking. The court was of the view that the latter 'has no long-term or permanent effect, so

[102] Reuben Binns and Michael Veale, 'Is that Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR,' *International Data Privacy Law* 11.4 (2021): 319–332.

[103] Wachter and Mittelstadt (n. 69) 584.

[104] Article 29 Working Party, 'ADM', 20.

that the automated decision has no legal consequences or significantly affects the drivers'.[105] A *strict* approach was hence taken by the ADC to interpreting the effect element of the Article 22 right, which is largely consistent with the A29WP guidelines that define the effect by reference to the exclusion of or discrimination against individuals.[106] The guidelines further consider the context of online advertising with specific criteria developed, but the lack of legal interpretation in a labour context, as has been discussed earlier, remains a gap to be filled.

iii. Right to Explanation

The *Uber/Ola* judgment has also rekindled the gridlocked debate on the right to explanation. Some believe that this right is neither existent nor does it have any practical relevance at all.[107] Yet, one major milestone of these Dutch rulings is the declaration that the drivers have access to personal data Ola uses to 'draw up the risk profile', along with information 'about segments into which applicants have been classified'.[108] The implications of *Uber/Ola* judgments for the right to explanation are mixed. First, as the conditions for Article 22 rights are difficult to satisfy (including the burden of proof), the associated 'right to explanation' grounded in Article 15(1)(h) is inoperable. Second, a distinction is made by ADC between the concept of automated decision-making and that of profiling, which often come in pairs under the GDPR. It is on such a basis the court held that there may be profile-based processing that involves no automation at all, and that the data subject may have a right 'to access the data used as input to create a profile', in accordance with Article 15(3) GDPR.[109] Hence, a more explicit recognition on the distinction between ADM and profiling creates space for a right to profile transparency. It might still be far from an ideal form of 'meaningful explanation' but, from the standpoint of building a data trust, such a recognition establishes another valid channel of data flow distinct from the previous ones.[110]

---

[105] *Uber Deactivation*, 4.25.

[106] Article 29 Working Party, 'ADM', 21-2.

[107] Raphaël Gellert, Marvin van Bekkum and Frederik Zuiderveen Borgesius, 'The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making,' EU Law Analysis, eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html.

[108] *Ola Access* (n. 52) 4.36, 4.45.

[109] *Ola Access* (n. 52) 4.35.

[110] Selbst and Powles (n. 101) 233.Wachter and Mittelstadt (n. 69) 494.

In sum, there are certainly positive developments from these judgments about each right, notably including the recognition of a right to profile transparency (based on Article 15 regardless of the involvement of automated decision-making), of rating portability (in an anonymised form), and of the ability to inspect and reverse automated dismissal. Such developments are instrumental in platform worker resistance but still fall short of building a union-backed data trust for workers. The EDPB has over the years developed a good number of guidelines related to data subject rights with a view to bringing clarity and suitability. However, little or nothing is said as to how these rights are distinct from each other and, in case of joint exercise of all data subject rights, what type and scope of data can be expected. Simply interpreting the GDPR provisions word by word is not enough, and several challenges (as identified in this chapter) are not duly anticipated and presented in the text of the GDPR. Efforts should be taken to update these guidelines with a view to engaging contextual and structural problems. A more holistic and comprehensive understanding of all these rights might be provided by updating the existing guidelines or by creating a new and overarching one that covers all rights horizontally. Further, the extent to which all the data subject rights under the GDPR overlap and interplay with each other remains understated and should have been properly addressed by guidelines at EU or national levels. The ADC rulings mark the absence of *horizontal* guidance that attends not just the specifics of a data subject right but its structural and instrumental role within the data subject rights system or the overall regime more generally. This might be fixed, it is argued, by re-adjusting the EDPB's priorities by providing holistic guidelines covering all the data subject rights as well as guidelines specifically about labour contexts. Given the presence of Article 88 expressly related, it is critical that the rights-based resistance this chapter reveals are not ignored or overshadowed for being paradigmatically different from the specific *protection* and *safeguards* for workers.

V. Macro-perspectives: Data Subject Rights as a Tool for Platform Worker Resistance

In addition to the challenges discussed above to each data right under the GDPR, this section considers a deeper issue as to whether these rights, taken as a whole, can be expected as a

reliable tool for platform worker resistance. The discussion is confined to the specific controversies arising out of the Dutch rulings, of which we identify three.

A. Victims of Information Asymmetries Bearing the Burden of Proof?

The existing commentaries on data subject rights as well as related guidelines from the EDPB and national DPAs have their focus primarily on substantial matters. The issue of how procedural rules may, in reality, constitute a barrier to effective use of data subject rights remains understated. We consider the allocation of the burden of proof only in this chapter, with other procedural aspects eg, the standard of proof, omitted as they are irrelevant to the Dutch rulings.

The concept of the burden of proof, also known as the 'probative burden', 'risk of non-persuasion', or the 'persuasive burden'[111] is self-explanatory. It refers to the obligation imposed on a party by a rule of law to adduce evidence in order to prove a fact in issue.[112] As most cases involve more than one issue, the legal burden may be distributed between the parties.[113]

This issue of the burden of proof is outstanding in the four Dutch rulings in which the judges impose the burden on the data subjects in many instances. From the outset, this may be justified by reference to the maxim that 'he who asserts must prove' (*ei incumbit probatio qui dicit, non qui negat*). The realities are, however, much more complex than this. Given the significant information asymmetries the drivers (as data subjects) suffer from, the need for considering the shifting and even reversal of the burden of proof is evident.

There may be some criticism against the court's reasoning that invariably places the onus on the drivers. According to civil procedural rules,[114] this is not necessarily unjustifiable. Generally speaking, the issue of which party bears the burden of proof in relation to any given fact is

---

[111] Adrian Keane and Paul Mckeown, *The Modern Law of Evidence* (Oxford: Oxford University Press, 2016), 80.

[112] Technically speaking, there is a distinction between legal burden and evidential burden (known also as the duty of passing the judge). The latter may not amount to a burden at all as it may be discharged by evidence 'other than the evidence adduced by the defence' Keane and McKeown (ibid), 80. This chapter focuses only on the former.

[113] Keane and McKeown (n. 111) 80.

[114] Note that the allocation of the burden of proof is different in criminal and civil cases, and this chapter focuses only on civil procedural rules.

determined by precedent, statutes or agreements. First, judges do not allocate the burden of proof based on any general principles. It is rather on precedents concerned with the issue of substantive law in question that the burden of proof is determined.[115] Second, the parties may expressly agree upon the incidence in some permissible cases (eg, written contracts). Beyond these cases, the burden of proof becomes the courts' construction. As Keane and McKeown contend, it is a matter of policy given the rule of substantive law in question.[116] Third, in some cases, the incidence may be directly determined by statute. The UK's Employment Rights Act 1996 requires the employer to show the reason for any dismissal, for instance. If the employer fails to provide a reason as such, the dismissal is deemed automatically unfair.[117]

The GDPR is almost silent on the burden of proof except for on some occasions – eg, Article 21 (on the right to object) and Article 12 (on manifestly unfounded or excessive requests). Per these Articles, the onus is *explicitly* placed on the controller to demonstrate either 'compelling legitimate grounds' for processing upon the data subject's objection or 'manifestly unfounded or excessive requests'. A more tentative claim can be made that data controllers are in various circumstances – such as Article 5 (the accountability principle), Articles 13–14 (information disclosure), Article 35 (data protection impact assessment) – put in the position to prove, demonstrate or provide information about the data processing or the use of automated decision-making systems not necessarily in the context of court proceedings. Therefore, much is left for domestic civil procedure law.

From a procedural perspective, shifting the burden of proof is a rather flexible scheme that does not remove all the burden from one party to another. It allows the plaintiff suffering from information asymmetries to meet a lesser burden or a lower degree than may be required, while giving the other party the possibility to rebut. It exists in areas where 'fault or evidence is difficult to pin down but society has a large interest in protecting plaintiffs'.[118]

---

[115] Keane and McKeown (n. 111) 79–116.

[116] Keane and McKeown (n. 111) 100.

[117] Employment Rights Act 1996, s 98.

[118] Legal Information Institute, 'Shifting the Burden of Proof,' www.law.cornell.edu/wex/shifting_the_burden_of_proof.

The exercise of data subject rights with a view to increasing transparency of data processing or algorithmic decision-making processes marks a prime case for burden shifting. Particularly in the work context, data subjects are in a disadvantaged position to solicit information and therefore deserve particular protection. A fairer procedural arrangement might be that, as a principle, the data subject seeking transparency and data access via the GDPR rights bears a limited and initial burden of proof; once discharged, it is then for the controller to disprove the fact. There may be more radical arrangements that the burden of proof is categorically reversed on to the data controller when it comes to the compliance of data subject rights. Giesen comments on some radical proposals in the European Group on Tort Law (EGTL) for the reverse of the burden of proof in case of proving fault (in the light of the gravity of the danger), enterprise liability and damage.[119] Inspiration may be obtained, for instance, from Article 4:201 EGTL that the burden is reversed if the general principle (he who asserts must prove) would result in 'unreasonable difficulties for that plaintiff due to the technical or organisational complexity of the defendant's activities)'.

It is outside the scope of this chapter to develop specific rules for placing the onus on a certain party. Yet, the case of shifting or reversing the burden of proof is direly needed in cases like the *Uber/Ola* judgments with the presence of power asymmetries. It is an irony that the drivers who exercise their data subject rights precisely for the reason of getting more information are required to provide information they do not have, and which they are seeking in the first place.The 'beneficiary pays' principle, allocating the burden to the plaintiff on default, should be critically reflected in the labour context as the parties involved are not equal in power relations. Platform workers who utilise their data subject rights to address information asymmetries merit particular protection, not only substantially but also *procedurally*. Such protection is neither afforded by labour protection law nor by data protection law.

Although the allocation of the burden of proof mostly lies with the court's discretion, there might arguably also be a critical role of the EDPB. Admittedly, the board is certainly not in a position to develop procedural rules for court proceedings, but the 'spirits' of data protection

[119] Ivo Giesen, 'The Reversal of the Burden of Proof in the Principles of European Tort Law: A Comparison with Dutch Tort Law and Civil Procedure Rules,' *Utrecht Law Review* 6.1 (2010): 22–32.

about tackling information and power asymmetries should be clearly expressed in the context of procedural justice and taken seriously by judges. In fact, the emphasis of the GDPR on the controller's duty to demonstrate (the accountability principle) and to ensure transparency implies that the GDPR actually contains unspoken procedural rules that should be articulated in the EDPB's guidelines.

B. Work-related Use of Data Subject Rights as Abusive?

In the *Uber/Ola* judgments, a particular claim was made by these platforms that the request for data access with a view to building a data trust instead of checking for data accuracy or processing lawfulness constitutes an abuse of right.

This term 'abuse of right' can be traced to the EU Charter of Fundamental Rights, Article 54 of which prevents activities 'aimed at the destruction of any of the rights and freedoms recognised in this Charter of at their limitation to a greater extent than is provided for herein'.[120] The abuse of right provision is presumably applicable to all the rights given to the fundamental right to data protection. It has been considered in the context of data protection, for instance, by AG Kokott in its opinion to *Nowak*.[121] Ausloos and Veale note that such a mechanism is 'rarely used, or at least not successfully, usually implicated in politically charged, high level issues concerning the freedom of expression or of associated, often when pitted against values of the defence of democracy'.[122] In their view, the abuse of rights issue is 'resolved' by empahsising the balancing of rights newly added to the GDPR, another issue to be discussed below. Indeed, such a defence was not successful in *Uber Access* and *Ola Access* as the ADC held that a data subject does not have to 'motivate or substantiate why he is making a request for access under the GDPR ... [or] show any particular interest or state the goal that he wants to achieve with the access'.[123]

---

[120] Charter of the Fundamental Rights of the European Union, Article 54.

[121] Case C-434/16 *Peter Nowak v Data Protection Commissioner*, Opinion of Advocate General Kokott, delivered on 20 July 2017, paras 42–50.

[122] Lorna Woods, 'Abuse of Rights', in *The EU Charter of Fundamental Rights: a Commentary*, eds. Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (London: Bloomsbury Publishing, 2021), 1545. Ausloos and Veale (n. 72) 302.

[123] *Ola Access* (n. 52) 4.4–4.7. *Uber Access* (n. 50) 4.24–4.26.

Data access denied on the basis of purpose mismatch is not trivial (particularly in the case of the right of access), and there might be room for strategic readjustment in future events. Should this tension not be resolved via creative and future-proof reading of the GDPR provisions, it would be reasonable to conclude that GDPR rights are not a proper vehicle for platform worker resistance, and that we should look for new legislative developments beyond this framework. Before a strategic turn, however, it is important to note that many requests were rejected not necessarily because of the inherent limitations, but due to misinterpretations, confusions and inconsistencies. This may be fixed in the appeal and/or via an updated guidance from data protection authorities, with a systematic rethinking of platform workers' situation and genuine needs. Indeed, a glimpse of hope is shown in the Dutch judgments that the court intends to detach from aged assumptions while attending to the novelty of new data subject rights.

C. Balancing of Rights as a Potential Barrier to Initiate Data Flows Towards Workers?

Both the rights of access and to data portability are subject to a balancing scheme, as per Article 15(4) and Article 20(4), which states that these rights should not adversely affect the rights and freedoms of others. According to the A29WP guidelines as well as Recital 63, these rights and freedoms include those of other data subjects (eg, customers of Uber and Ola) as well as those of the controller.[124] In contrast to what the names of these rights literally indicate (ie, access and portability), the balancing scheme may constitute a serious impediment to data flows away from data controllers.

The consideration of third-party privacy (mostly that of Uber/Ola customers) in the balancing act has rendered a variety of data inaccessible via Articles 15 and 20 GDPR, including GPS data, customer 'reports' as well as passenger details. A somewhat inconsistent finding was made, however, about ratings, arguably one of the most valuable datasets for workers. In the *Ola/Uber Access* judgments, it was held that the platform should provide ratings in an anonymous form.[125] While access to ratings is generally commendable, two main issues may

[124] Article 29 Working Party, 'Right to Data Portability', 10–11.

[125] *Ola Access* (n. 52) 4.25. *Uber Access* (n. 50) 4.51–4.52.

arise from the Dutch rulings: first, the court fails to consider the possibility of providing access to, or portability of, the requested data other than ratings in an anonymised form. Second, the court does not make explicit the legal basis on which such an anonymised access is granted and the potential implications of anonymisation techniques for data reusability. The fact that the ADC judgments open up a ground with reference to anonymisation techniques on which privacy and utility can be better balanced is commendable. However, without detailed and effective guidance from the court or related authorities, it leaves a range of questions unanswered, eg, what exact technique of anonymisation should be used and deemed GDPR-compliant, whether anonymised data can be re-used by the drivers in their data trust, and the extent to which privacy risks can be mitigated by the mandated anonymisation.

Moreover, the ADC also balances the drivers' data access rights with those of the platforms. In this regard, platforms claim that providing data would give the drivers insights into its anti-fraud detection systems. According to the A29WP guidelines, however, a potential business risk cannot in and of itself serve as a basis for refusing any portability request.[126] Presumably, an anti-fraud defence would not be strong enough to dismiss access or portability requests. The ADC did not perform any substantial analysis but relied again upon the burden of proof, this time imposed on the platforms. The failure to substantiate their anti-fraud claims with further information made the court rule in favour of the drivers, thereby removing another anticipated barrier to initiate data flows towards the platform workers.[127]

In sum, the general and procedural issues mentioned above have significant implications for the effective enforcement of the right to data protection but remain understated in the data protection scholarship. While authorities are committed to developing rules around the principle of accountability, little is done from the court's perspective, for instance, in establishing connection between procedural rules and the essence of data protection. Indeed, uncertainty about the GDPR provisions cannot be solely clarified by judges as authorities at different levels are expected to do more heavy lifting. However, there is and should be a critical and distinctive role for the court to ensure that such general and procedural matters do not constitute undue barriers to the exercise of data subject rights.

---

[126] Article 29 Working Party, 'Right to Data Portability', 12.

[127] *Ola Access* (n. 52) 4.46. *Uber Access* (n. 50) 4.67.

VI. Future Developments: Data Rights Vis-à-Vis Other Legal Developments

The GDPR's general approach does not always adequately address power and informational asymmetries that are inherent in an employment relationship, as well as the lack of collective rights. Article 88 of the GDPR is an opening which allows for Member States to provide 'more specific rules' on data protection in the workplace.[128] However, many Member States have not done so.[129] Even in cases where Article 88 was mentioned, it seems to be a marginal point.[130] A pending case at the Administrative Court of Wiesbaden and potential developments in Germany may alter this. As Abraha, Silberman and Adams-Prassl argue, the opportunity which Article 88 offers is underutilised, but the development of Article 88 laws must create more specific rules, rather than duplicate existing GDPR requirements.[131]

Other developments are more positive, specific and attentive directly to platform workers. Chapter III of the proposed EU Directive on Platform Work (in the trialogue stage at the time of writing), for instance, provides some improvements to the GDPR in addressing algorithmic management. Most significantly, Articles 6–8 improve transparency by ensuring that workers have a right to explanation by a contact person of the platform company for any decisions taken or supported by an ADM which 'restrict, suspend or terminate the platform worker's account [...] refuse the remuneration for work performed by the platform worker, [...] affect the platform worker's contractual status or any decision with similar effects'.[132] Worker representatives will also be enabled to access information about automated systems, and overall strengthen

---

[128] GDPR Art 88. See also Halefom H. Abraha, 'A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace,' *International Data Privacy Law* (2022): 7, doi.org/10.1093/idpl/ipac015.

[129] Justin Nogarede, *No Digitalisation Without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace* (Brussels: FEPS, 2021), feps-europe.eu/publication/826-no-digitalisation-without-representation/.

[130] In Italy: case number/name 9669974 (Municipality of Bolzano). Case number/name 9685994 (Deliveroo). Case number/name 9518890 (Gaypa s.r.l.). In Germany: Case number/name2 A 124/22 (OVG Saarlouis). Case number/name10 Sa 2130/19 (LAG Berlin-Brandenburg).

[131] Halefom H. Abraha, Michael Silberman and Jeremias Adams-Prassl, 'The Need for Employee-specific Data Protection Law: Potential Lessons from Germany for the EU,' *European Law Blog*, europeanlawblog.eu/2022/09/30/the-need-for-employee-specific-data-protection-law-potential-lessons-from-germany-for-the-eu/.

[132] Proposed EU Directive on Platform Work Art 8(1).

collective consultation rights (but not collective bargaining).[133] The protection afforded by Articles 6–7 will apply to *all* platform workers, even those that fall outside of an employment relationship (Article 10). Overall, the chapter is certainly an improvement on some collective rights, better protection on personal data collection and transparency into automated monitoring and decision-making systems. However, the Directive still adopts a techno-solutionist approach to algorithmic management, assuming that these systems and practices are acceptable, simply because there is available technology to do so. Whether and the extent to which these protections will be watered down in the trialogue process is yet to be determined, and how it will interact with the proposed AI Act has become a cause of concern.[134] The proposed AI Act classifies some AI systems in the employment context as high-risk, which entails these high-risk systems complying with stricter requirements.[135] However, there are shortcomings to it that do not particularly take sufficient account of the power and informational asymmetries in a work context.[136] Essentially as a model of product regulation, the AI Act regulates users and developers but fails to provide a framework for rights and redress to empower those who are affected by AI technologies. While these new legislative proposals are crucial and necessary developments, the GDPR remains useful since its universal rights-based framework applies to a wider set of workers and work contexts beyond the platform economy.

VII. Conclusion

The Dutch rulings are not the endgame as these cases are under appeal at the time of writing. Yet, a detailed analysis of them gives a glimpse of how these rights are tied to the logic of lawfulness or accuracy, thereby being distant from the ideas of data utility, flow and analytics. The rulings highlight a structural tension that the practical value of data subject rights is not

---

[133] Proposed EU Directive on Platform Work Art 6(4).

[134] Valerio de Stefano and Antonio Aloisi, 'Artificial Intelligence and Workers' Rights,' *Social Europe*, socialeurope.eu/artificial-intelligence-and-workers-rights/.

[135] Proposed AI Act Annex III 4(a), 4(b).

[136] ibid. Aude Cefaliello and Miriam Kullmann, 'Offering False Security: How the Draft Artificial Intelligence Act Undermines Fundamental Workers Rights,' *European Labour Law Journal* (2022): 2–4. doi-org.proxy.uba.uva.nl/10.1177/20319525221114474.

well envisioned or anticipated by legislators. While not explicitly stated in the GDPR contexts, these rights are constrained by the court's teleological and restrictive reading deeply rooted in the Luxemburg jurisprudence. What the drivers explicitly and intentionally pursue, ie to drive and pool personal data into a data trust operated by the Worker Info Exchange, is rife with challenges and uncertainties.

In the digital society, courts must confront this reality of unconventional, creative use of data rights and respond with certainty whether they are permissive or not, sometimes requiring a stretch of the GDPR provisions. It appears, from a global perspective, that courts tend to be more permissive, with the purpose-related constraints removed in some jurisdictions, and new rights defined without necessarily adhering to conventional interpretation. This is a welcome development, but a more thorough and systematic reflection is urgently needed. The four judgments constitute a good start, but are far from initiating a valid and systematic dialogue on the configuration and facilitation of data subject rights in reality. It is of prime importance judges revisit some deeply rooted assumptions developed in the last century and ask critical fundamental questions: what is the role of intent or purpose in determining the scope and nature of data rights? Whether and exactly how may anonymisation techniques lawfully facilitate data flows and mitigate privacy and security concerns? Should procedural matters be developed in line with the spirits of the fundamental right to data protection, particularly with reference to the principle of accountability and the overarching objective of addressing information and power imbalances? It is hoped that these fundamental questions will be properly addressed in the appeal, making the Dutch cases the beginning rather than the end of rights-based platform worker resistance.

References

Abraha, Halefom H. 'A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace.' *International Data Privacy Law* (2022): 1–21. doi. org/10.1093/idpl/ipac015.

Abraha, Halefom H., Michael Silberman and Jeremias Adams-Prassl. 'The Need for Employee-specific Data Protection Law: Potential Lessons from Germany for the EU.' *European Law Blog*, 30 September 2022. europeanlawblog.eu/2022/09/30/the-need-for-employee-specific-data-protection-law-potential-lessons-from-germany-for-the-eu/.

Acevedo, Deepa Das. 'Regulating Employment Relationships in the Sharing Economy.' *Employee Rights and Employment Policy Journal* 20 (2016): 1–35.

Adams-Prassl, Jeremias. 'What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work.' *Comparative Labor Law and Policy Journal* 41, no. 1 (2019): 123–146.

Ada Lovelace Institute. Exploring Legal Mechanisms for Data Stewardship. London: Ada Lovelace Institute, 2021. www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.

Aloisi, Antonio and Valerio de Stefano. *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour*. London: Bloomsbury Publishers, 2022.

Altenried, Moritz. 'Mobile Workers, Contingent Labour: Migration, the Gig Economy and the Multiplication of Labour.' *Environment and Planning A: Economy and Space* (2021): 1–16.

Anwar, Mohammad, A. and Mark Graham. 'Between a rock and a hard place: Freedom, flexibility, precarity and vulnerability in the gig economy in Africa.' *Competition & Change* 25, no. 2 (2020): 237–258.

Article 29 Working Party. 'Guidelines on the Right to Data Portability.' WP242, rev.01.

Aslam, Yaseen and Jamie Woodcock. 'A History of Uber Organizing in the UK.' *South Atlantic Quarterly* 119, no. 2 (April 2020): 412–421.

Ausloos, Jef, René Mahieu and Michael Veale. 'Getting Data Subject Rights: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance.' *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10, no. 1. (2019): 283–309.

Ausloos, Jef and Michael Veale. 'Researching with Data Rights.' *Technology and Regulation* (2021): 136–57.

Binns, Reuben and Michael Veale. 'Is that Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR.' *International Data Privacy Law* 11, no. 4 (2021): 319–332.

Buolamwini, Joy and Timnit Gebru. 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.' In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81 (2018): 77–91. proceedings.mlr.press/v81/buolamwini18a.html.

Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press, 1992.

Bessa, Ioulia, Simon Joyce, Denis Neumann, Mark Stuart, Vera Trappmann and Charles Umney. *A global analysis of worker protest in digital labour platforms*. Geneva: International Labour Organiation, 2022. www.ilo.org/wcmsp5/groups/public/---dgreports/---inst/documents/publication/wcms_849215.pdf.

Bygrave, Lee A. 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling.' *Computer Law & Security Review* 17, no. 1 (2001): 17–24.

Cano, Melissa R., Ricard Espelt and Mayo Fuster Morell. 'Flexibility and freedom for whom? Precarity, freedom and flexibility in on-demand food delivery.' *Work organisation, labour & globalisation* 15, no. 1 (2021): 46–68.

Cant, Callum. *Riding for Deliveroo: Resistance in the New Economy*. Cambridge: Polity, 2020.

Cant, Callum and Jamie Woodcock. 'Fast Food Shutdown: From Disorganisation to Action in the Service Sector.' *Capital & Class* 44, no. 4 (2020): 513–521. doi.org/10.1177/0309816820906357.

Casilli, Antonio A. 'Digital Labor Studies Go Global: Toward a Digital Decolonial Turn.' *International Journal of Communication* 11 (2017): 3934–3954. ijoc.org/index.php/ijoc/article/download/6349/2149.

Cefaliello, Aude and Miriam Kullmann. 'Offering False Security: How the Draft Artificial Intelligence Act Undermines Fundamental Workers Rights.' *European Labour Law Journal* (2022): 1–21. doi-org.proxy.uba.uva.nl/10.1177/20319525221114474.

Chen, Julie Yujie. 'Thrown under the Bus and Outrunning It! The Logic of Didi and Taxi Drivers' Labour and Activism in the on-Demand Economy.' *New Media & Society* 20, no. 8 (2018): 2691–2711. doi.org/10.1177/1461444817729149.

Clarke, Laurie. 'Data is the Next Frontier in the Fight for Gig Workers' Rights.' *Tech Monitor*, 24 March 2021. techmonitor.ai/policy/education-and-employment/data-next-frontier-fight-for-gig-workers-rights.

Colclough, Christina. 'Towards Workers' Data Collectives.' *IT for Change*, January 2021. projects.itforchange.net/digital-new-deal/2020/10/22/towards-workers-data-collectives/.

Collier, Ruth Berins, Veena B. Dubal and Christopher L. Carter. 'Disrupting Regulation, Regulating Disruption: The Politics of Uber in the United States.' *Perspectives on Politics* 16, no. 4 (2018): 919–937. doi.org/10.1017/S1537592718001093.

de Sousa Santos, Boaventura. 'Law: A Map of Misreading. Toward a Postmodern Conception of Law.' *Journal of Law and Society* 14, no. 3. (1987): 279–302. doi.org/10.2307/1410186.

de Stefano, Valerio. 'The Rise of the 'Just-in-Time Workforce': On-Demand Work, Crowdwork, and Labor Protection in the "Gig-Economy."' *Comparative Labor Law and Policy Journal* 37, no. 3 (2016): 471–504.

——, '"Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work.' *The International Journal of Comparative Labour Law and Industrial Relations* 36, no. 4 (2020): 425–443. doi.org/10.54648/ijcl2020022.

de Stefano, Valerio and Antonio Aloisi. 'European legal framework for digital labour platforms'. *Publications Office of the European Union*, (2018): 1–66. doi:10.2760/78590.

——, 'Artificial Intelligence and Workers' Rights.' *Social Europe*, 8 November 2021. socialeurope.eu/artificial-intelligence-and-workers-rights.

Dencik, Lina. 'Towards Data Justice Unionism? A Labour Perspective on AI Governance.' In *AI for Everyone: Critical Perspectives*, edited by Pieter Verdegem, 267–284. Westminster: University of Westminster Press, 2021. doi.org/10.16997/book55.o.

Dubal, Veena B. 'Winning the Battle, Losing the War?: Assessing the Impact of Misclassification Litigation on Workers in the Gig Economy.' *Wisconsin Law Review*, no. 4 (2017): 739–802.

——, 'The New Racial Wage Code.' Harvard Law and Policy Review 15, no. 2 (2021): 511–550.

EDPB. 'Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre.' *EDPB*, 2 October 2020. edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en.

——, 'Riders: Italian SA Says No to Algorithms Causing Discrimination: A platform in the Glovo group fined EUR 2.6 million.' *EDPB*, 5 July 2021. edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en.

——, 'The Icelandic DPA has fined a company running ice cream parlours for processing employee's personal data via video surveillance camera installed in an employee area.' *EDPB*, 29 June 2021. edpb.europa.eu/news/national-news/2021/icelandic-dpa-has-fined-company-running-ice-cream-parlours-processing_en.

——, 'Guidelines 01/2022on Data Subject Rights - Right of Access.'

Edwards, Lilian and Michael Veale. 'Slave to the Algorithm? Why A Right to Explanation Is Probably Not the Remedy You Are Looking For.' *Duke Law & Technology Review* 16, no. 1 (2017): 18–84.

European Commission. 'Commission Staff Working Paper GDPR Impact Assessment.' SEC/2012/0072 final.

Gandini, Alessandro. 'Labour Process Theory and the Gig Economy.' *Human relations* 72, no. 6 (2019): 1039–1056.

Gellert, Raphaël, Marvin van Bekkum and Frederik Zuiderveen Borgesius. 'The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making.' EU Law Analysis. eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html.

Gig CV. 'About GigCV.' gigcv.org/.

Giesen, Ivo. 'The Reversal of the Burden of Proof in the Principles of European Tort Law: A Comparison with Dutch Tort Law and Civil Procedure Rules.' *Utrecht Law Review* 6, no.1 (2010): 22–32.

Goodman, Bryce and Seth Flaxman. 'European Union Regulations on Algorithmic Decision-making and a 'Right to Explanation.' *AI magazine* 38, no. 3 (2017): 50–57.

Gregory, Karen. '"Worker Data Science" Can Teach Us How to Fix the Gig Economy.' *WIRED*, 7 December 2021. www.wired.com/story/labor-organizing-unions-worker-algorithms/.

——, '"My Life is More Valuable Than This": Understanding Risk among On-Demand Food Couriers in Edinburgh.' *Work, Employment and Society* 35, no. 2 (2020): 316–331.

Hallinan, Dara. Borgesius, Frederik Zuiderveen. 'Opinions Can Be Incorrect (in Our Opinion)! On Data Protection law's Accuracy Principle.' *International Data Privacy Law* 10, issue 1 (2020): 1–10.

Hießl, Christina. 'Case law on algorithmic management at the workplace: Cross-European comparative analysis and tentative conclusions.' *European Commission, Directorate DG Employment, Social Affairs and Inclusion.* (September 2021): 1–25. papers.ssrn.com/sol3/papers.cfm?abstract_id=3982735.

Irani, Lilly C. and Michael Six Silberman. 'Turkopticon: Interrupting Worker Invisibility in Amazon Mechanical Turk'. In *CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (April 2013): 611–620.

Jędrzej, Niklas and Lina Dencik. 'What rights matter? Examining the place of social rights in the EU's artificial intelligence policy debate.' *Internet Policy Review* 10, no. 3 (2021): 20–23. doi.org/10.14763/2021.3.1579.

Johnston, Hannah and Chris Land-Kazlauskas. *Organizing On-Demand: Representation, Voice, and Collective Bargaining in the Gig Economy.* Geneva: International Labour Orgaisation Conditions of Work and Employment Series, no. 94. (2019): 1–41. www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_624286.pdf.

Kaminski, Margot E. 'The Right to Explanation, Explained.' *Berkeley Technology Law Review* 34 (2019): 189.

Keane, Adrian and Paul Mckeown. *The Modern Law of Evidence.* Oxford: Oxford University Press, 2016.

Lata, Lutfun N., Jasmine Burdon and Tim Reddel. 'New tech, old exploitation: Gig economy, algorithmic control and migrant labour.' *Sociology Compass* (2022): 1–14.

Legal Information Institute. 'Shifting the Burden of Proof.' www.law.cornell.edu/wex/shifting_the_burden_of_proof.

Lobel, Orly. 'The Law of the Platform.' *Minnesota Law Review* 137 (2016): 87–166.

Lomas, Natasha. 'Dutch Court Rejects Uber Drivers' "Robo-Firing" Charge but Tells Ola to Explain Algo-Deductions.' *TechCrunch.* techcrunch.com/2021/03/12/dutch-court-rejects-uber-drivers-robo-firing-charge-but-tells-ola-to-explain-algo-deductions/.

Lynskey, Orla. *The Foundations of EU Data Protection Law.* Oxford: Oxford University Press, 2015.

Mahieu, René, Hadi Asghari and Michel van Eeten. 'Collectively exercising the right of access: individual effort, societal effect.' *Internet Policy Review* 7, no. 3 (2018): 1–23.

Mahieu, René and Jef Ausloos. 'Harnessing the collective potential of GDPR access rights: towards an ecology of transparency.' *Internet Policy Review*, (2020). policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487.

Malgieri, Gianclaudio. 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations.' *Computer Law and Security Review* 35, no. 5 (2019).

Mazur, Joanna. 'Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law,' *Erasmus Law Review*, 11 (2018): 178–189.

Mendoza and Lee A. Bygrave, 'The Right Not to Be Subject to Automated Decisions based on Profiling,' in *EU Internet Law*, edited by Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou, 77–98. Cham: Springer, 2017.

Möhlmann, Mareike and Lior Zalmanson. 'Hands on the wheel: navigating algorithmic management and Uber drivers' autonomy.' In *Proceedings of the International Conference on Information Systems (ICIS) Seoul, South Korea*, (December 2017): 1–17. www.researchgate.net/publication/319965259_Hands_on_the_wheel_Navigating_algorithmic_management_and_Uber_drivers'_autonomy.

Moore, Phoebe, Martin Upchurch and Xanthe Whittaker. 'Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism.' In *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, eds. Phoebe Moore, Martin Upchurch and Xanthe Whittaker, 1–16. Cham: Palgrave Macmillan, 2018.

Nogarede, Justin. *No Digitalisation Without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace*. Brussels: FEPS, 2021. feps-europe.eu/publication/826-no-digitalisation-without-representation/.

Pandey, Akshat and Aylin Caliskan. 'Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms.' In *AIES 2021 – Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, (July 2021): 822–833. doi.org/10.1145/3461702.3462561.

Purtova, Nadezhda. 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law.' *Law, Innovation and Technology* 10, no. 1 (2018): 40–81.

Popan, Cosmin. 'Algorithmic Governance in the Gig Economy: Entrepreneurialism and solidarity among food delivery workers.' In *Cycling Societies: Innovations, Inequalities and Governance*, edited by Dennis Zuev, Katerina Psarikidou and Cosmin Popan.

Rogers, Brishen. 'The Law and Political Economy of Workplace Technological Change.' *Harvard Civil Rights-Civil Liberties Law Review* 55, no. 2 (2020): 531–584.

Safak, Cansu and James Farrar. *Managed by Bots: Data-Driven Exploitation in the Gig Economy*. London: Worker Info Exchange, 2021. www.workerinfoexchange.org/wie-report-managed-by-bots.

Scholz, Trebor. 'Introduction: Why does digital labor matter now?' In *Digital Labor: The Internet as a Playground and Factory*, edited by Trebor Scholz, 1–10. New York: Routledge, 2012.

Selbst, Andrew D. and Julia Powles. 'Meaningful Information and the Right to Explanation.' *International Data Privacy Law* 7, no. 4 (2017): 233–42.

Stefflbauer, Nakeema. 'When Human rights + Digital rights = Workers' rights.' *Digital Freedom Fund*, 2 May 2022. digitalfreedomfund.org/when-human-rights-digital-rights-workers-rights/.

Tassinari, Arianna and Vincenzo Maccarrone. 'Riders on the Storm: Workplace Solidarity Among Gig Economy Couriers in Italy and the UK.' *Work, Employment and Society* 34, no. 1 (2020): 35–54. doi.org/10.1177/0950017019862954.

Terranova, Tiziana. 'Free Labor: Producing Culture for the Digital Economy.' *Social Text* 18, no. 2 (2000): 33–58. muse.jhu.edu/article/31873.

Toh, Jill. 'UK gig drivers recognised as workers – what next?' *Social Europe*, 25 February 2021. socialeurope.eu/uk-gig-drivers-recognised-as-workers-what-next.

Tosoni, Luca. 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22 (1) of the General Data Protection Regulation.' *International Data Privacy Law* 11, no. 2, (2021): 145–162.

Vallance, Chris. 'Legal action over alleged Uber facial verification bias.' *BBC*, 8 October 2021. www.bbc.com/news/technology-58831373.

van Doorn, Niels. 'At What Price? Labour Politics and Calculative Power Struggles in on-Demand Food Delivery.' Work organisation, Labour & Globalisation 14, no. 1 (2020): 136–149. doi:10.13169/workorgalaboglob.14.1.0136.

van Doorn, Niels and Julie Yujie Chen. 'Odds stacked against workers: datafied gamification on Chinese and American food delivery platforms.' *Socio-Economic Review* 19, no. 4. (2021): 1345–1367.

Veale, Michael. 'A Better Data Access Request Template.' michae.lv/access-template/.

Veale, Michael and Lilian Edwards. 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-making and Profiling.' *Computer Law & Security Review* 34 (2018): 398–404.

Wachter, Sandra and Brent Mittelstadt. 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI.' *Columbia Business Law Review* 2 (2019): 443, 499.

Wachter, Sandra, Brent Mittelstadt and Luciano Floridi. 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation.' *International Data Privacy Law* 7, no. 2 (2018): 76–99.

Wong, Benjamin. 'Delimiting the Concept of Personal Data after the GDPR.' *Legal Studies* 39, no. 3 (2019): 517–532.

Woods, Lorna. 'Abuse of Rights.' In *The EU Charter of Fundamental Rights: A Commentary*, edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, 1545. London: Bloomsbury Publishing, 2021.

Woodcock, Jamie and Mark Graham. *The Gig Economy: A Critical Introduction*. Cambridge: Polity Press, 2020.

Worker Info Exchange. 'About WIE.' www.workerinfoexchange.org/.

Zanfir-Fortuna, Gabriela. 'Right of Access by the Data Subject.' In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechesler, 449–468. New York: Oxford University Press, 2020.