Agosti, Claudio; Bronowicka, Joanna; Polidoro, Alessandro; Priori, Gaetano

Research Report

Exercising workers' rights in algorithmic management systems: Lessons learned from the Glovo-Foodinho digital labour platform case

Report, No. 2023.11

Provided in Cooperation with:
European Trade Union Institute (ETUI), Brussels

Suggested Citation: Agosti, Claudio; Bronowicka, Joanna; Polidoro, Alessandro; Priori, Gaetano (2023) : Exercising workers' rights in algorithmic management systems: Lessons learned from the Glovo-Foodinho digital labour platform case, Report, No. 2023.11, ISBN 978-2-87452-690-9, European Trade Union Institute (ETUI), Brussels

This Version is available at:
https://hdl.handle.net/10419/300310

Exercising workers' rights in algorithmic management systems

Lessons learned from the Glovo-Foodinho digital labour platform case

Claudio Agosti, Joanna Bronowicka, Alessandro Polidoro and Gaetano Priori

Report 2023.11

etui.

Exercising workers' rights in algorithmic management systems

Lessons learned from the Glovo-Foodinho digital labour platform case

Claudio Agosti, Joanna Bronowicka, Alessandro Polidoro and Gaetano Priori

Report 2023.11
european trade union institute

Claudio Agosti is the founder of Tracking Exposed and an algorithm analyst.

Joanna Bronowicka is a sociologist and a researcher at the Center for Interdisciplinary Labour Law Studies at the European University Viadrina.

Alessandro Polidoro is a certified lawyer and the head of legal of Tracking Exposed.

Gaetani Priori is a computer security specialist in Tracking Exposed.

Brussels, 2023

Print: ETUI Printshop, Brussels

D/2023/10.574/27
ISBN: 978-2-87452-689-3 (print version)
ISBN: 978-2-87452-690-9 (electronic version)

The ETUI is co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the ETUI. Neither the European Union nor the ETUI can be held responsible for them.

Contents

Executive summary

In July 2021, the Italian Data Protection Authority fined Foodinho, the Italian subsidiary of the Spanish food delivery company Glovo 2,600,000 euros for failing to protect the digital rights of its workers. The Italian authority ordered the company to comply with obligations listed in the GDPR, to check whether the algorithmic management systems used to control its workforce were fair and accurate, and to prevent discriminatory outcomes.

At the time of this landmark decision, the Tracking Exposed team was preparing its first technical investigation into the mobile app used by Glovo in Italy. The investigation revealed that the app tracked riders' locations, even outside their working hours, and shared their location data and other categories of data with third parties, including marketing companies.

The system used by Glovo is an example of algorithmic management, a form of management coming under increasing scrutiny due to the challenges that the use of algorithms can pose to human rights in general, and workers' right in particular. In this report, we analyse the importance of the Glovo case for the enforcement of workers' digital rights, demonstrating how technical experts, data protection authorities and trade unions can join forces to collect evidence about workplaces deploying algorithmic management.

We start by demonstrating the significance of the decision of the Italian data protection authority to fine a platform company for violating Art. 22 GDPR in an employment context. This decision shows the critical role that data protection authorities can play in uncovering problems with automated processing at the workplace, and in enforcing workers' digital rights. Fulfilling this role, however, requires effective cross-border cooperation as well as resources for conducting technical audits of management systems.

We go on to present how workers or their representatives can use technical methods to collect evidence about platform companies using mobile apps to manage workers. By deploying the 'black-box testing' method, we were able to reveal which data was shared by the app with the platform during and outside the working hours. This inexpensive method of auditing apps could be used by experts working for trade unions to quickly verify whether an app used by a company is compliant with data protection laws.

Indeed, we believe that technical experts may hold the key to the black box of algorithmic management. Trade unions are in a unique position to facilitate

cooperation between technical experts and workers, and to support projects documenting the challenges posed by algorithmic management to workers' rights.

Collecting evidence about algorithmic management is critical for workers seeking to enforce their rights by filing complaints with national DPAs or competent courts. The availability of technical expertise can also help improve workers' negotiating positions in a collective bargaining context. Ultimately, we believe that, by helping workers understand the apps that control them, we can give them the key to unlock their rights and build a fairer future of work for all.

Foreword

Automated decision-making and monitoring systems are disrupting working conditions, and not in a manner beneficial to workers. This report examines AI systems used to mediate work though digital labour platforms. From both a practical and worker protection perspective, accessing and challenging these systems is difficult as the overall architecture of the algorithmic process. When confronted with opaque models, access to information is essential to exercise rights. Indeed, who would not want better access and a better understanding of the so-called 'black-box' systems?

The aims of this report are a) to provide evidence on how to exercise GDPR rights in the context of platform work, and b) to strengthen workers' ability to exercise their digital rights in workplaces subject to algorithmic management, i.e., relying on automated decision-making and monitoring systems. More concretely, the authors suggest that raising complaints with the competent Data Protection Authority (DPA) enables technical investigations to be carried out, thereby producing technical and non-technical evidence.

Although numerous studies exist on the topic, they vary in quality and usefulness. While studies on algorithmic management abound in the literature, most provide no technical analysis. The jurisprudence on platforms is another important source of evidence, albeit quite fragmented. Technical expertise thus plays a key role and is an important and needed component of any comprehensive analysis, as now recognised by data protection authorities. Covering this aspect in relation to a recent DPA case in Italy, this report comprises four parts.

The first part analyses the Italian DPA's decision to sanction the developers of the Glovo Courier app, in this case Glovo, a Spanish company operating in Italy through its subsidiary Foodinho. It highlights the role of the DPA as the competent authority in charge of supervising implementation of data protection law.

The decision known as *'Order no. 234 against Foodinho s.r.l.'* is of key importance in the labour context. It marks the first time that a data protection authority has fined a company for violating GDPR Article 22 in the employment context, a provision that relates to algorithmic management. It identifies two elements of algorithmic management, namely the 'Excellence Score' and remote workforce management, as evidence of the platform's control.

The decision also finds that other GDPR rights and obligations have been violated: the principles of lawful processing of data, transparency, 'privacy by design' and

'privacy by default'; the security of processing; the requirement to conduct a data protection impact assessment; as well as the obligation to designate a Data Protection Officer.

The DPA's decision confirms that riders should be considered as employees of the digital labour platform, decision in line with similar decisions of Italian courts.

The lesson here is that, by addressing cases involving algorithmic management, DPAs and the courts can clarify how social and human rights are impacted by automated decision-making. However, to do so, DPAs need the expertise of other competent authorities, including labour inspectorates responsible for overseeing labour issues.

The second part describes the technical investigation carried out by experts on the app installed on the phone of an individual platform worker. A form of reverse engineering, the method used was 'black-box testing' which allows people with technical expertise to literally see the data that has been collected and accessed by the digital labour platform through the app and processed by algorithmic management. The method does not involve accessing the source code: one can see what goes into or comes out of the algorithmic black box, without needing to open it or look into it. The evidence gathered shows not only how a worker was 'managed' when performing his work, but also how workers' rights, including the right to privacy, are being potentially violated. Performing this investigation required the collaboration of the individual worker: the process to be used was explained to him in depth, his informed consent was gained, and all communication with him was subject to confidentiality.

The third part presents the technical analysis of the Glovo Courier app for one user, conducted by 'Tracking Exposed', a project which gathered technical evidence subsequently submitted to the DPA through a reporting procedure. The aim of the analysis was to respond to four research questions:

- Question 1: Does the Glovo Courier app track riders' locations outside their working hours?
- Question 2: What categories of data does the Glovo Courier app share with the platform outside riders' working hours?
- Question 3: Does the Glovo Courier app share personal data with third parties not mentioned in the privacy policy?
- Question 4: Does the Glovo Courier app process any additional form of scoring unknown to the rider?

The team of experts carried out the technical analysis twice, with a view to gathering evidence of any changes to the app over time, and showing which violations occurred when.

Finally, the report shares lessons learned about the use of such a technical analysis, a potential solution to overcoming the lack of transparency and cooperation shown by digital labour platforms. Based on reverse engineering, the technical investigation enabled the researcher to observe the actual behaviour of the software component governing the worker's activities behind the app's

interface. The researcher inspected the data communicated by the app to the company's IT system, and observed when the system dispatched orders. A lot of new evidence was gained from this analysis. While some, such as the summary of completed orders or a calendar to book future shifts, were to be expected, others were less expected, such as the presence of a hidden metric named 'Excellence Score'. Interestingly, this documented the fact that, when the app is running in the background, it continues to send frequent notifications of orders to all riders, even those not on shift, leading to the hypothesis that the app tracks a rider's behaviour even when off duty.

This report is a landmark study describing and demonstrating how automated decision-making and monitoring systems work, with a focus on the concrete inputs and outputs of algorithmic decisions. Through their technical analysis, the experts in charge were able to observe what personal data was collected from the mobile phone and whether this data was transferred to third parties. Hopefully, this report will help trade unions and workers' representatives to better understand that expert advice is available and that there are ways to gather technical and non-technical evidence of violations to workers' privacy, data protection and fundamental rights.

Aida Ponce Del Castillo
Senior researcher, European Trade Union Institute (ETUI), March 2023

Introduction

New challenges to workers' rights

Frank promised to be more like a supportive friend than an unfair manager. Yet, a court in Bologna found that Frank was not fair at all – in fact, he discriminated against couriers delivering food for a platform company by assigning better orders to those he liked.[1] Frank was not a human manager, but an algorithm created by a company called Deliveroo. The Bologna court ruling constituted a historic victory for the Italian trade union CGIL and a landmark case on the use of algorithmic management (Aloisi and De Stefano 2021). Indeed, algorithmic management is coming under increasing scrutiny as it represents the challenges that the use of algorithms can pose to human rights in general, and workers' right in particular.

In this report, we sketch an alternative path for workers wanting to access their rights in workplaces governed by algorithmic management. Rather than taking a company to court, this path involves filing a complaint with a data protection authority (DPA) responsible for enforcing the EU's General Data Protection Regulation (GDPR). We show that collecting technical evidence of how workers' data is accessed, collected, and processed by platforms can be the first step in protecting their rights. We demonstrate that technical investigations can be conducted not only by data protection authorities, but also by independent experts. Ultimately, we encourage trade unions and other workers' representatives to become more proactive in cooperating with technical experts and data protection authorities to collect evidence of data protection violations, with a view to strengthening protection of workers' rights.

The debate on workers' rights in digitalised workplaces was accelerated by the Covid-19 pandemic, with many workers compelled to work from home questioning the use of remote monitoring tools. However, the use of technology for workplace monitoring or surveillance is not new. In fact, it has a long history, and can be seen as the key element of the capitalist mode of production (Thompson 2003). However, recent technological developments, such as Internet and email monitoring, location tracking, covert surveillance, and the processing of personal data, have resulted in new challenges to privacy and other human rights at work (Ball 2010).

---

1. Tribunale Ordinario di Bologna, Decision no. 2949/2019, 27.11.2020.

The Covid-19 pandemic put 'platform workers' delivering food on bikes, motorcycles or in cars in the spotlight. These platform workers, often referred to as 'riders', were deemed vital to the economy alongside doctors, nurses, teachers or bus drivers. However, unlike these other professionals, riders are often not classified as employees, but rather as self-employed 'partners' of the platform companies. This not only denies them full access to workers' rights, but also from collective bargaining coverage.

Moreover, digital labour platforms rely on algorithms to supervise, monitor and control workers. The use of such algorithms is under intense scrutiny from researchers and policymakers. Platform companies have become the focus of the debate over workers' rights in digitalised workplaces. This report contributes to this debate by demonstrating how technical evidence can be used to unravel the functioning of such algorithms and strengthen cooperation between all those interested in protecting workers' rights.

1. Goals of the report

The overarching goal of this report is to demonstrate the role that technical evidence can play in protecting workers' rights. In particular, we hope to demonstrate how technical experts, data protection authorities and trade unions can cooperate to collect evidence of data protection violations and strengthen the protection of workers' rights in workplaces using algorithmic management.

In the first part of the report, we highlight the role that data protection authorities can play in protecting workers' rights by analysing the decision of the Italian DPA to fine the producers of the Glovo Couriers app, in this case Glovo, a Spanish company operating in Italy through its subsidiary Foodinho. The Italian DPA's decision, formally called Order no. 234 of 10 June 2021, details the numerous data protection violations revealed by a thorough examination of the algorithmic management deployed by the company. This *ex officio* investigation relied on technical evidence collected by Italian DPA officials, as well as evidence obtained through cooperation with the Spanish Data Protection Authority (AEPD). We consider this decision a landmark ruling, as to our knowledge it is the first time that a data protection authority has fined a company for violating Art. 22 GDPR[2] in an employment context.

In the second part of the report, we show how to collect technical evidence from the mobile apps used by platform companies. We present the results of our own pilot study, conducted via the 'black-box testing' method, into the Glovo Couriers app. This technical analysis revealed that the app tracked riders' locations, even outside their working hours, and shared their location data and other categories of data with third parties, including marketing companies. While we acknowledge that this method alone cannot be used to draw conclusions about data protection violations, we consider it extremely useful for workers and their representatives to gain quick insights into which worker data is being accessed, collected and shared with the platform. By revealing which categories of data are collected by the platform, it can also help flag risks associated with algorithmic management, for example algorithmic bias. We hope to inspire other technical experts to deploy this method in other companies working with mobile apps.

---

2. Art. 22 GDPR Automated individual decision-making, including profiling. '1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'

In the third part of the report, we consider the lessons learned from the Glovo case which are applicable in the context of other platforms and companies using algorithmic management. The main lesson is that closer cooperation between technical experts, data protection authorities and trade unions can strengthen enforcement of workers' rights. We believe that trade unions are in a unique position to facilitate cooperation between technical experts and workers, and to support projects documenting challenges to data protection rules at work. We hope to encourage trade unions to use data protection laws and institutions to defend workers' rights as an alternative to courts and collective bargaining procedures.

The conclusion contributes to the broader debate over challenges to the enforcement of the GDPR in an employment context, and proposals for new solutions able to strengthen workers' rights.

1.1 Research on algorithms in the workplace

In recent years, the topic of algorithms at work has benefited from growing research interest in a variety of disciplines (Ajunwa 2018; Kellogg et al. 2020; Bernhardt et al.2021). Defined in the broadest sense, algorithms are 'encoded procedures for transforming input data into a desired output, based on specified calculations' (Gillespie 2014). Algorithms are increasingly being used to automate decision-making in the workplace, despite evidence that algorithmic bias can exacerbate existing inequalities (Barocas and Selbst 2016), for example, precluding people with certain characteristics from being hired (Ajunwa 2020). In addition to discrimination, potential dangers generated by automated decision-making include work intensification, deskilling, lower wages and less economic mobility, contingent work, suppression of the right to organise, and loss of privacy, autonomy and dignity (Bernhardt et al. 2021).

Digital labour platform companies rely heavily on algorithms for mediating, supervising and organising work (Prassl and Risak 2015; Kocher 2022). The interaction between automated systems and humans in such workplaces constitutes what is described as an 'algorithmic management' regime with 'the unique ability to track worker behaviour, constantly evaluate performance with rewards and penalties and automatically implement decisions. Algorithmic management provides the feeling of working with a 'system' rather than humans, and is characterised by lower transparency (in most cases).' (Moehlmann and Zalmanson 2017). To protect human rights in automated decision-making systems, it is fundamentally important that humans be kept in the loop about how these systems function, and have the discretion to change automated decisions, as well as sufficient time and proper training to asses them (Wagner 2019). Improving the transparency and accountability of algorithms does not necessarily involve accessing the source code – as this can be particularly difficult to obtain in the case of private companies – but can also be achieved by looking at the external inputs and outputs of a decision-making process, rather than at its inner workings (Edwards and Veale 2017; Kroll et al. 2017).

Lacking access to technical evidence about algorithmic management, social scientists have focused on its consequences for workers. Algorithms can exacerbate already precarious working conditions characterised by unpredictable scheduling, fluctuating earnings, and unreliable long-term employment prospects, by adding distinctly 'digital' aspects, such as data-driven performance and a lack of algorithm transparency (Bronowicka and Ivanova 2021). Confronted with an opaque system of management, workers sometimes resort to constructing theories, stories and urban legends about how algorithms work (Moehlmann and Zalmanson 2017), leading to scholars coining such terms as 'allegorithm' (Anderson 2016) or 'algorithmic imaginary' (Chan and Humphreys 2018).

However, research into algorithms at work would benefit from more technical evidence demonstrating how algorithmic management works, including the inputs and outputs of algorithmic decisions. The growing jurisprudence on platform companies is fragmented, with court decisions only describing certain elements of algorithmic management. The key research issue is thus how to obtain technical evidence that can be used to study algorithms at work without the cooperation of the company deploying them. In our view, one way is to look at the mobile apps that platform workers install on their phones.

1.2 Mobile app analysis – a key to the black box?

'A new global privacy emergency is called the app economy' – said the head of the Italian Data Protection Authority (DPA) in January 2019 (Soro 2019). Indeed, mobile apps often access, collect and share user data, enabling companies to capture and monetise people's behaviours (Zuboff 2019). By introducing mobile apps to the world of work, platforms such as Uber or Deliveroo have blurred the line dividing consumers and workers. With the ability to integrate behaviour at work into a consumer profile, advertisers can now gain a full picture not only of what we buy, but also when we work or rest.

Riders working for platforms are usually required to install a company's mobile app on their private phones. The app collects large amounts of data throughout the whole working process. Some of this data is provided knowingly, for example by a rider swiping his screen to confirm an order has been delivered (Ivanova et al. 2018). However, the app can also observe riders' behaviour without their knowledge, for example by tracking their exact location.

Platform companies use their mobile apps to collect provided and observed data and automatically send it to their IT systems for further processing. In other words, automated decisions are not made by the app, but by a company's IT system based on data collected by the app. Without the cooperation of the company involved, one cannot scrutinise either the source code of the mobile app or the higher-level IT system, which is why they are considered to be a 'black box'.

When we started investigating platform companies in 2020, we realised that apps offer an interesting vantage point for innovative research. Our team at Tracking Exposed, a not-for-profit, free software project, had already been putting a

spotlight on user tracking and profiling, on the data market and on the influence of algorithms in other sectors. The team consisted of experts in new technologies and information security, as well as lawyers with expertise in data protection law.[3] We realised that the fact that mobile apps are installed on private phones is advantageous for deploying our research methods in a new context of work.

Inspired by exchanges with the experts of the ETUI's Foresight Unit to pursue this research, we decided to conduct a pilot study on an app used by a platform company in Italy. We designed a method using 'black-box testing', an approach commonly used in the information security industry and which is affordable, quick and easy to replicate. The method allows technical experts to see which data is accessed and collected by the app without accessing its source code. Moreover, it reveals which data is shared with the platform and is thus a candidate for being processed by an algorithm. In other words, we can see what enters or exits the black box without looking inside it.

We wanted to see whether this method could deliver technical evidence of security and privacy issues in platform companies. In particular, we wanted to know whether the apps collect and share data beyond what is agreed with the riders and what is legally allowed under the GDPR. When we were ready to launch our pilot study of the first app, Glovo Courier, in summer 2021, we learned that the Italian DPA had issued a historical decision, fining the makers of the app 2.6 million euros for data protection violations.[4]

The Italian DPA's decision encouraged us to pursue our research further, as it highlighted the importance of technical evidence for enforcing workers' rights. The need for technical expertise was further emphasised by the recent call issued by the European Data Protection Board (EDPB), the EU body contributing to the consistent application of data protection rules and promoting cooperation between data protection authorities in Europe.[5] The call clarifies the key areas of technical expertise in new technologies and information security, unsurprisingly including skills necessary for analysing mobile apps. In our view, technical experts may be holding the key to the black box of algorithmic management, opening a new door to understanding the future of workers' rights.

---

3. More about the Tracking Exposed project: https://tracking.exposed

4. Garante per la Protezione dei Dati Personali (2021), Ordinanza ingiunzione nei confronti di Foodinho s.r.l., Registro dei provvedimenti n. 234, 10.06.2021.

5. European Data Protection Board. Call for Expressions of Interest, Establishment of a List of Individual Experts for the implementation of the EDPB's Support Pool of Experts, 21.2.2022. https://edpb.europa.eu/our-work-tools/our-documents/call-expressions-interest-experts-implementation-edpbs-support-pool_en

2. Analysis of the Italian Data Protection Authority's Order no. 234

In this section, we discuss the context, content and importance of the decision of the Italian Data Protection Authority (DPA) to fine a platform company for non-compliance with the GDPR.

In July 2019, this authority, called in Italian the *Garante per la Protezione dei Dati Personali*, launched an investigation into Foodinho, the Italian subsidiary of the Spanish food delivery company Glovo. In June 2020, the Spanish DPA, the *Agencia Española de Protección de Datos* (AEDP), concluded its own investigation of Glovo with a decision to fine the company 25000 euros for non-compliance with its duty to appoint a Data Protection Officer, as per Art. 37 GDPR.[6]

A year later, the Italian DPA fined Glovo's subsidiary Foodinho 2,600,000 euros for non-compliance with several GDPR articles. Issued on 10 June 2021, the 44-page decision, formally known as Order no. 234, details the investigation, the exchange of substantive and legal arguments between Foodinho and the DPA, the cooperation with the Spanish DPA, the final conclusions of the proceedings and the remedies and penalties imposed on the platform.[7]

The Italian DPA accompanied the publication of the decision with a shorter abstract in English summarising the numerous GDPR infringements. The company was ordered to comply with obligations listed in the GDPR, including taking 'suitable measures to safeguard the data subject's rights, fundamental freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision, with regard to the automated processing performed via the platform including profiling (Article 58(2)(d) GDPR)', 'suitable measures to regularly check fairness and accuracy of the results of algorithmic systems, partly in order to ensure that the risk of errors is minimised and to comply with Section 47-d of legislative decree No 81/2015 as for the prohibition to discriminate, access to and exclusion from the platform (Article 58(2)(d) GDPR)', and 'suitable measures to introduce arrangements that can prevent inappropriate and/or discriminatory applications of feedback-based reputational mechanisms; this assessment will

---

6. Agencia Española de Protección de Datos (2020), Procedimiento Nº: PS/00417/2019 – Resolució de Pro-cedimento Sancionador, 09.06.2020. https://www.aepd.es/es/documento/ps-00417-2019.pdf

7. Garante per la Protezione dei Dati Personali (2021), Ordinanza ingiunzione nei confronti di Foodinho s.r.l., Registro dei provvedimenti n. 234, 10.06.2021. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9675440

have to be performed each time the algorithm is changed as for the use of feedback information to calculate the scoring (Article 58(2)(d) GDPR)'.[8]

Moreover, the Italian DPA ordered the company to comply with provisions set forth in Art. 4 of the Italian Workers Statute. This is important for two reasons. First, it unequivocally points to the fact that the DPA considered the riders to be workers whose data rights were infringed 'as part of the relevant employer-employee relations in breach of the applicable employment laws regulating remote surveillance of employees'. Second, the decision is a reminder of an important feature of Italian law – the fact that data protection rights and labour laws have been implemented jointly in an employment context.

The platform appealed the Italian DPA's decision at the Tribunal of Milan arguing that the fine is excessive and in conflict with Art. 83 GDPR. The Tribunal agreed with Foodinho and overturned the entire decision in November 2022, not just the extent of the fine.[9] The Italian DPA is now challenging the ruling of the Tribunal in the Italian Supreme Court (*Corte di Cassazione*). At the time of writing this report, the decision of the Supreme Court (the final instance in this case) is still pending.

2.1 Legal framework in Italy

The DPA's decision needs to be considered in the context of Italy's data protection laws and labour laws. To sanction the unlawful use of surveillance technology in the workplace in Italy, a court must enforce these two laws jointly. How data protection and labour laws interact differs from one EU country to another. This is a result of the flexibility clause in Art. 88 GDPR that allows Member States to adopt more specific rules on the processing of employees' personal data, either by law or collective agreements.

In Italy, the two laws needing to be jointly implemented to sanction the unlawful use of technology for monitoring work activity are the Workers Statute (*Statuto dei Lavoratori*) and the Data Protection Code (*Codice della Privacy*). Specifically, Art. 4 of the Workers Statute regulates the remote control of employees by means of 'audiovisual equipment and other control instruments' during their working hours. Dating back to 1970, the Workers Statute represented a turning point in industrial and labour relations in Italy and is considered to be a very progressive piece of legislation that proved to be ahead of its time in many ways (Grandi and Pettinelli 2020).

In addition to norms concerning the freedom and dignity of workers, employment and trade unions, the Statute includes provisions specifically designed to address the challenges posed by the use of technology in the workplace. Even though

---

8. Garante per la Protezione dei Dati Personali (2021) Abstract of Italian SA's order as issued against Foo-dinho S.r.l., 05/07/21. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677611

9. 'Annullata la sanzione del Garante privacy a Foodihno (Glovo) per 2.6 milioni di euro.' https://www.lawtalks.it/annullata-la-sanzione-del-garante-privacy-a-foodihno/

such equipment was not commonplace in 1970, the lawmakers wanted to pre-empt any excessive use of surveillance devices, already deemed as endangering workers' rights. Workers did not want their performance to be assessed by a distant company manager through an invisible control mechanism. For this reason, Article 4 generally prohibits the use of audiovisual equipment and other instruments that can be used to remotely control workers' activity, with only few specific exceptions. The idea behind this rule was to avoid creating an unbalanced power relationship between employees and an employer by allowing the latter to use excessive means of surveillance (Grandi and Pettinelli 2020).

Moreover, Art 4 introduced a still-existing procedural guarantee: the use of any remote control tools has first to be explicitly authorised either by the representatives of the trade unions active in the company or, in case of their absence, by the National Labour Inspectorate.

The more recent development of the data protection laws in Italy, on the other hand, was prompted by the Personal Data Directive adopted by the European Union in 1995.[10] The Italian Data Protection Authority was established in 1996[11], while the Italian Code of Personal Data Protection was adopted in 2003.[12] The Code contains provisions dedicated to data processing within an employment relationship. In its Art. 114 about the remote control of workers, the Code explicitly refers to the Italian Workers Statute, stating that 'the provisions of Article 4 of Law no. 300 of 20 May 1970 remain in effect'. Moreover, Article 171 of the Code refers to Articles 4 and 38 of the Statute, stating that any non-compliance with the prohibition of worker's remote control perpetrated with malicious intent shall be considered a violation and punished accordingly.

After the GDPR come into force in 2018, both the Workers Statue and the Code of Personal Data Protection were updated to expand data protection in an employment context.[13] The current version of Art. 4(3) of the Statute states that the information collected by the employer through remote control means can be used for all purposes related to the employment relationship only if the employee has received in advance adequate information on how this control will be carried out, pursuant to the provisions of the Italian Code of Personal Data Protection.

---

10. Directive 95/46/EC of the European Parliament and of the Council 'On the protection of individuals with regard to the processing of personal data and on the free movement of such data', 24.10.95.

11. Law no. 675 of the Italian Republic 'Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali', 31.12.96.

12. Legislative Decree nr. 196 of the Italian Republic 'Codice in materia di protezione dei dati personali', 30.06.03.

13. Legislative Decree nr. 101 of the Italian Republic 'Disposizioni per l'adeguamento della normativa nazio-nale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 apri-le 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, non-che' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE', 04.07.18.

2.2 Challenges of the Italian framework

While these legal developments created a robust legal framework for protecting data rights in an employment context, the interpretation of these laws is not shared unanimously among scholars and practitioners, generating a certain level of legal uncertainty. In fact, the lack of stability seems to be a more general problem impacting Italian labour law as a whole (Vallebona 2020). This uncertainty is also caused by a lack of decisive jurisprudence and the difficulties encountered during collective bargaining procedures when dealing with complex technological issues.

Over the past few years, significant progress has been made in recognising platform-based food delivery workers as employees, and thus giving them access to the full set of labour rights, including the right to bargain collectively. In 2019, Italian lawmakers amended a provision introduced in 2015, extending employment and labour protection to platform workers, unless a collective agreement provided otherwise. In January 2020, the Italian Supreme Court's judgement applied this law, ruling in favour of Foodora riders suing their platform (Aloisi and De Stefano 2020). In November 2020, the Tribunal of Palermo reclassified a Glovo rider as a subordinate employee, recognising a standard employment relationship between a worker and a platform for the first time in Italy (De Stefano et al. 2021). In February 2021, a prosecutor in Milan ordered four platforms, Uber Eats, Just Eat, Deliveroo and Foodinho-Glovo to reclassify 60,000 riders and pay a total of 733 million euros in fines (Parodi 2021).

In addition to ruling on the nature of the employment relationship, the Italian courts also play an important role in interpreting core legal principles in the context of rapidly developing new technologies. However, changes of perspective may significantly transform the content of a norm, in turn leading to uncertainty over how certain rules will be applied in future. For example, the meaning of Article 4 of the Workers Statute has evolved, prompted by the 2002 ruling of the Italian Supreme Court. This ruling introduced the concept of 'defensive control', justifying the use of technical instruments even without a worker's knowledge or observing authorisation procedures, when they are intended to ensure the 'safety' of means of production when the latter are subject to aggression from employees.[14] Such a ruling clearly represented a shift in favour of the employer and opened the door to decisions less favourable to workers. For example, in 2014 the Italian Supreme Court recognised an employer's right to create a fake Facebook profile to check on his workers and verify their behaviour.[15]

The trade unions can also play a key role in defining norms on the use of technology in the workplace by making use of collective bargaining procedures. After a collective agreement is concluded, it is considered on a par with primary law. In practice, pay and working time remain the most common subjects of collective bargaining, with only few collective agreements explicitly addressing

14. Suprema Corte di Cassazione (2002), decision nr. 4746, department of labour law, 03.04.02 17.

15. Suprema Corte di Cassazione (2015), decision nr. 10955, department of labour law, 25.05.15.

the use of technology. For instance, subjects like smart-working practices or the implementation of artificial intelligence at the workplace are yet to be properly addressed within these procedures. Since the ability of workers to co-define rules concerning technology is a right that is rarely taken up, the impact of collective agreements on improving legal certainty has thus been ambivalent.

In this context of legal uncertainty, the Italian DPA has played a key role in establishing a path forward by issuing guidelines, opinions and orders. As an administrative body with supervisory powers, it oversees implementation of data protection laws – also in an employment context. It can provide informed opinions when requested or issue official guidelines, such as those regulating workplace surveillance via video cameras or email monitoring tools.[16] Importantly, the DPA can reply to complaints from data subjects or launch *ex officio* investigations, without the involvement of the data subject concerned. Specifically, data subjects in Italy may address their concerns to the DPA in two ways: either via a formal complaint pursuant to Art. 77 GDPR, or via an official report (*Segnalazione*) pursuant to Art. 144 of the Italian Code of Personal Data Protection.

By issuing binding decisions, known as Orders, the DPA can contribute to enforcing data protection rights, including those of workers. The technical and legal expertise gained in other cases in other sectors can be applied in the employment context. Being an administrative body, the DPA does not formally belong to the judiciary, instead serving as an aid for justice matters and interpreting norms strictly related to the protection of personal data. This means that the strategic litigation efforts of workers and their representatives can be extended beyond the courts to include national DPAs. However, as we will demonstrate in this report, the investigations into algorithmic management involve significant human, financial and technical resources.

2.3 The Italian DPA's investigation of Glovo

The full text of the Order gives us insights into how the Italian DPA conducted its investigation into Glovo and the methods it used to collect evidence.[17] This *ex officio* investigation started in July 2019 when DPA inspectors arrived at Foodinho's headquarters without prior notice. The inspectors used the company's computers to access the interface used for workforce management called 'Admin Platform'. It immediately became clear to them that the amount of data displayed greatly exceeded what it should have been. For instance, the inspectors found out that, from that very office in Italy, 'it was possible to verify that the platform allows the visualisation of riders' data in all countries where Glovo is active (even outside

16. Garante per la Protezione dei Dati Personali (2007), Lavoro: le linee guida del Garante per posta elettroni-ca e internet, 01.03.07. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1387522 & also Garante per la Protezione dei Dati Personali (2010), Provvedimento in materia di videosorveglian-za, 08.04.10. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1712680

17. Garante per la Protezione dei Dati Personali (2021), Ordinanza ingiunzione nei confronti di Foodinho s.r.l., Registro dei provvedimenti n. 234, 10.06.2021. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9675440

the EU) by selecting 'Country of choice' from a drop-down menu, showing the same details as for riders of one's own country' (pg. 3).

The inspectors also asked for access to the company's legal and technical documentation related to data protection law compliance. In August 2019, the company submitted several documents, including descriptions of the algorithm used to assign orders to riders and the one used to establish riders' scores, as well as the architecture of the platform's rider management system.

The Italian DPA soon noticed that certain documents submitted by Glovo were incomplete or inconsistent with each other. For example, the company submitted two different versions of the information document for workers required by Art. 13 GDPR – one during the inspection and a second one later in a separate legal statement. Immediately spotting the discrepancies between the two, the DPA deemed neither version to be sufficient, while also noting that there was no indication as to when they had been drafted. As stated in the Order with regard to the second version: 'Examining this information document – that does not show a date and of which the company has not provided any indication on when it was drafted – some modifications emerge when compared with the model provided during the inspection. However, for this new information document too, some elements seem non-compliant, as described above, with the principles imposed by Art. 5 and demanded by Art. 13 GDPR' (pg. 18).

In addition to directly collecting evidence at the company's headquarters, and to the documentation requested from the company, the Italian DPA also turned to its counterpart in Spain to assist with the investigation of Glovo and Foodinho. First, the Italian DPA initiated a cooperation procedure with the Spanish DPA pursuant to Art. 56 GDPR to verify which one was the competent authority. The Spanish DPA agreed on assigning competence to the Italian DPA with regard to the processing activities performed by Foodinho S.r.l., as these substantially affected riders working in Italy on the basis of an employment contract with this company. Three documents transmitted by the Spanish DPA were used in arriving at the decision in the Italian case.

On November 2020 the Italian DPA concluded its investigation. It notified Foodinho of the detected GDPR violations and any necessary remedies. For several months, the platform had the opportunity to submit further arguments in its favour, albeit without succeeding in convincing the DPA. The many statements made by the company during the proceedings were insufficient to justify the lack of compliance and, according to the DPA, Foodinho was not very cooperative, as stated in the Order: 'the company cooperated with the Authority only partially during the proceedings' (pg. 42).

2.4 Analysis of the decision

The DPA investigation culminated in a historic decision, formally known as 'Order no. 234 against Foodinho s.r.l.' issued on 10 June 2021.

The company was found guilty of violating seven different GDPR articles: Art. 5.1 (a), (c) and (e), Art. 13, Art. 22, Art. 25, Art. 30, Art. 32, Art. 35 and Art. 37.

Some of the charges referred directly to clear infringements of the main principles of European data protection law laid down in Art. 5 GDPR. The *principle of transparency* was considered violated due to the fact that the platform never offered complete information about the processing of such relevant data as the messages and recorded phone-calls between riders and the company support centre. The fact that proper information was not provided to the workers or the DPA was also interpreted as a failure to comply with the *principle of fairness*.

The design and security of the technical system used by Glovo's subsidiary was deemed at odds with the *principle of data minimisation*, because it made the data of riders in different countries available to anyone with access to the Admin Platform. The data retention period, in most cases four years after the end of the work contract, was deemed excessive and unlawful. Moreover, the Italian DPA found that riders' data was exposed to the risk of leaks, alteration or unlawful access as the cyber-security measures had not been updated since the system's introduction in 2016.

The information notice and privacy policy drafted by Foodinho, under Glovo's direction, were deemed to be too broad and generic, and not satisfying the rights of data subjects. The data processing records required by Art. 30 GDPR lacked crucial information such as the duration of data retention or security measures. The contact details of the Data Protection Officer were only made available to the public in July 2020.

Furthermore, the DPA ruled that Glovo was indeed supposed to draft and submit a Data Protection Impact Assessment, even though the company claimed it was not necessary (pg. 18). In this respect, the Italian DPA was extremely clear: 'The company has not carried out a data protection impact assessment as required of the data controller by Art. 35 of the Regulation following the recognition of the processing carried out. [...] the innovative nature of the technology used by the company (including the application to be installed on the rider's device and the geolocation functionality) - and the consequent high risk for the rights and freedoms of data subjects - is evident from the examination of the functioning of the digital platform around which the activity carried out by Foodinho Srl revolves' (pg. 25-28).

Crucially, the decision of the Italian DPA reveals that Glovo has *de facto* created a fully automated workforce management system, described as follows: 'the company carries out, through the whole system used for the operation of the platform, automated processing, including profiling, as part of the so-called 'Excellence System' whereby it assigns each rider, through the application of

specific and predetermined parameters, a score that allows priority access to the 'system for selecting the time slots' established by the company' (pg. 28). Glovo relied on an algorithm for calculating riders' 'Excellence Score', which was then fed into another automated system called Jarvis used for assigning orders. In other words, the algorithmic management system decided automatically which riders should be assigned better orders, and which should be given worse ones, based on their previous performance. There was no human supervision involved in making these decisions, and riders were unable to challenge them – they could only accept an order or reject it.

Concerning the use of the algorithmic management system, the Italian DPA detected violations of Art. 22 GDPR. Specifically, it found that Glovo had not implemented any 'measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention'. Though the company tried to undermine or even deny the existence of any automated decision-making based on the processing of riders' data, the Italian DPA was clear on this point: 'Differently to what is claimed by the company, the required setting of the parameters on the basis of the functioning of the algorithm does not negate per se the possibility to take decisions based solely on automated processing' (pg. 28).

Last but not the least, the DPA decision confirmed that riders should be considered as employees, in line with the recent rulings of Italian courts. The Italian DPA deemed the geolocation tracking to be unlawful as it violated Art. 4 of the Workers Statute and the related norms. The decision also refers to other elements of the algorithmic management system, such as its Excellence Score and remote workforce management, as evidence of the platform's control, thereby supporting the reclassification of riders as employees.[18] The company's rebuttal that its riders were autonomous freelancers was not accepted by the DPA: 'Although the company has not fully clarified under which formulas and mechanisms the algorithms that govern the overall functioning of the digital platform operate, [...] it manages the entire execution phase of the order' (pg. 35-36). From this basis it was possible to assess the nature of the riders' employment relationship: 'Examination of the concrete processing performed reveals that, regardless of what is abstractly stated in the employment contract, the riders continuously perform the work through mainly personal activities and in a manner substantially determined and organised by the company also through the use of the digital platform. [...] While performing – via a range of technological tools (the digital platform, the app and the channels used by customer care) – data processing which allows the meticulous control of the work performed by the riders, the company has failed to apply what is established by the aforementioned art. 4, paragraph 1, l. 300/1970'(pg. 37-39). With this decision, the DPA also implies that robust compliance with data protection rules could help clarify how algorithmic management systems affect working conditions, thus contributing more broadly to protecting workers' rights.

18. Tribunale di Palermo (2020), Decision no. 3570, 22.11.2020.

2.5 The importance of the decision

In issuing this decision, the Italian DPA has shown that national data protection authorities can play a key role in protecting and enforcing workers' rights. It has demonstrated to its European counterparts that effective investigations into platform companies can be conducted *ex officio*, as well as highlighting the use of collecting evidence and cooperating with DPAs in other Member States. We can only hope that the Italian DPA's case will be the first of many such initiatives, with other national DPAs soon following suit.

To our knowledge, the Italian DPA's decision was the first time that a DPA has fined a company for infringing Art. 22 GDPR in an employment context. Previous decisions in this context were taken by courts – most notably, the Amsterdam District Court which required the platform company Ola to explain the logic behind a fully automated decision.[19] This was the first time that a European court qualified an algorithmic decision as an automated decision in the sense of Art. 22 GDPR (Safak and Farrar 2021). In another case however, the same Amsterdam court agreed with Uber's argument that the platform did not use automated decision-making in the sense of Art. 22 GDPR.[20]

It appears that platform companies have become the testing ground for the enforcement of Art. 22 GDPR for courts and DPAs alike. This is certainly a new field for the DPAs, though they have made several attempts to investigate cases of automated decision-making in other contexts – for example the Portuguese DPA when it ordered an educational institution to stop using a proctoring app to evaluate students online, because it could lead to discriminatory results.[21] However, it seems that workers as data subjects in an employment context are serving well as case studies to test the limits of the current provisions. In other words, by considering cases involving algorithmic management at work, courts and DPAs are helping clarify our human rights in other spheres of life affected by automated decision-making and artificial intelligence.

---

19. Rechtbank Amsterdam (2021), Zaaknummer C / 13/689705 / HA RK 20-258, 11-03-2021. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019

20. Rechtbank Amsterdam (2021), Zaaknummer C/13/687315 / HA RK 20-207, 11.03.21. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020

21. Comissão Nacional de Proteção de Dados (2021), Deliberação/2021/622, 28.05.21. https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887 & more example of decisions concerning Article 22 in this section of GDPRhub.eu: https://gdprhub.eu/index.php?title=Category:Article_22_GDPR

3. Analysis of the Glovo Courier mobile app

In this chapter, we present the results of an analysis of the Glovo Courier app conducted by technical experts belonging to the Tracking Exposed project. The analysis was conducted in three phases: the first in July to September 2021, the second in February 2022, and the third in July 2022. In all three cases, the black-box testing method was applied to the same user of the Glovo Courier app.

The evidence collected in the first analysis pointed to several potential data protection violations, including tracking the location of riders outside their working hours and sharing extensive geolocation data with the Glovo platform and other companies. The second analysis pointed to the evidence of data protection violations not being conclusive, suggesting that the company might have taken steps to comply with the Italian DPA's decision.

The technical evidence collected in this pilot study was submitted to the DPA through a reporting procedure known as a *Segnalazione*. This procedure was helpful in our case as it does not need require a complaint to be filed by a data subject, although it is not binding for the authority. We hope that this evidence will be useful in further evaluations of whether Glovo is compliant with GDPR rules, but also more broadly in strengthening cooperation between technical experts and DPAs. Finally, we hope that it can be used by trade unions and other workers' representatives wishing to conduct similar investigations into apps used by platforms and other companies which rely on algorithmic management systems.

3.1 Research context

This research was initiated in 2020 when the Tracking Exposed project team became interested in the topic of platform companies using mobile apps for algorithmic management systems. In July 2021, we were ready to launch our technical investigation into the Glovo Courier app. By coincidence, the Italian DPA issued a decision that same month pertaining to the company we intended to study. We saw this as an opportunity to compare the results of our investigation with those of the Italian DPA.

The first step of this pilot study was to conduct a survey of platform workers. With the support of Italian lawyer Stefano Rossetti from the privacy organisation

NOYB,[22] we developed a questionnaire for workers around their experience with automated decision-making (Annex A). The Italian version of the questionnaire was first made available in July 2020, but yielded only one response.[23] Thanks to a collaboration with the Investigative Reporting Project Italy (IRPI), the questionnaire was published in both Italian and English on their whistleblowing platform.[24] By January 2022, the questionnaire had been filled out by 20 more riders from three different companies operating in Italy.

As a second step, we needed to establish direct communications with at least one rider interested in cooperating in the mobile app analysis. The last question of the survey stated: 'To successfully organise possible collective lawsuits against digital platforms that violate workers' rights, we may need your help. If you are interested, leave us your email.' We reached out to a rider who provided his email and who worked for Foodinho, the Glovo subsidiary in Italy.

In principle, anyone can download a Glovo Courier app, though only a verified rider can log into the app. We conducted our analysis with the participation of the rider who contacted us and consented to it. The latter involved many hours of conversations in which we established trust, explained the goals of the research, and detailed the mobile app analysis process, including a guarantee of anonymity. We were helped by the fact that the technical experts had connections to an informal riders' organisation. Furthermore, since the rider already planned to terminate his cooperation with Glovo, he had no fear of reprisals from the company in the event of his participation being revealed.

One lesson learned from this process is that this type of cooperation between riders and technical experts can benefit from the involvement of trade unions or other workers' representatives who have already established riders' trust. The importance of technical analysis should be framed in terms of the goals that the particular group of workers is trying to achieve, with these goals possibly varying from one group to another. Trade unions and other workers' representatives can play an important role in reaching out directly to workers interested in participating in such technical analyses, explaining the process and the purpose of such investigations, developing adequate consent procedures and disseminating the results to public authorities, researchers or policymakers.

3.2 Basic user experience analysis

We started by conducting a basic user experience analysis, reproducing the steps a rider needs to take to download, install and use the app on his phone. We downloaded the Glovo Courier app available for Android users (a similar app with

22. My Privacy is None of Your Business, https://noyb.eu/en
23. The Italian version was initially accessible on the website: https://riders.want.their.tracking.exposed/
24. Riders e Food delivery https://irpimedia.irpi.eu/diventa-una-fonte/irpileaks/ (English questionnaire in https://framaforms.org/lifes-a-game-food-delivery-and-riders-1633514624).

a slightly different name exists for Apple devices).[25] When riders download the app from a virtual store, for example the Google Play Store, they are informed that they consent to the terms and conditions available under the link to the company website. This link leads the user to a document containing the General Terms of Use and Contracting in many languages. A further hyperlink calls up a document called Privacy and Data Protection Policy.[26] As these documents are the same for customers and couriers alike, they include no information explicitly concerning a worker's data.

Thanks to the rider's participation, we were able to see the general design of the app's user interface. The app displays available orders, a summary of completed orders, as well as a calendar feature to book future shifts. It also displays the 'Excellence Score'. As the participating rider had an Excellence Score of 0, the shift-booking feature was not available.

When a rider finishes a shift, he can log off the app, close it, or do both. The default behaviour of many app users is to leave multiple apps running in the background. We noticed that, when the app is running in the background, it continues to send notifications of unassigned orders to all riders, even those not on a shift, sometimes as often as every hour. These notifications would not appear if the rider logged off or closed the app. According to the rider participating in our study, the company encouraged riders to leave the app running in the background, so they would be notified about orders even outside their shifts. It was however unclear whether accepting or rejecting these orders would impact their 'Excellence Score' or other performance metrics.

The fact that such notifications would appear when the Glovo Courier app was left running in the background led us to hypothesise that the app was tracking rider behaviour, including their geolocation, even outside working hours. We suspected that a more in-depth analysis of the app might reveal the amount of data accessed, collected and processed, and even reveal traces of automated decision-making. We decided to perform black-box testing on the app to answer the following research questions.

Research Question 1: Does the Glovo Courier app track riders' locations outside their working hours?
Research Question 2: What categories of data does the Glovo Courier app share with the platform outside riders' working hours?
Research Question 3: Does the Glovo Courier app share personal data with third parties not mentioned in the privacy policy?
Research Question 4: Does the Glovo Courier app perform any form of scoring unknown to the rider within the platform or with other parties?

These questions are answered individually in Section 3.4.

---

25. Version for Apple users is called Glovo Couriers.
26. https://glovoapp.com/en/legal/privacy-couriers/

3.3 The black-box testing method

To answer these research questions, we used a method of mobile app analysis called 'black-box testing'.[27] The first analysis was conducted over the course of three weeks – partly in July, partly in September 2021. The analysis was then repeated over the course of two weeks in February 2022, and one week in July 2022 (methodology in Annex B and C, findings in Annex D).

The first analysis was on the app version 2.92.0, the second on version 2.120.0, and the third on version 2.146.0.

Though this type of analysis does not allow experts to see *inside* the black box, thereby gaining full knowledge of how the application works, it does allow them to observe from the outside how the black box interacts with the user's mobile phone and other parties. In particular, it allows us to record and study which data the app *collects* from the mobile phone and which data is *sent* to the network.

For example, through this type of black box testing, we can check whether a mobile application records and sends the content of conversations at certain times. This can be observed in two ways: when the application turns the microphone on and off, and through the presence of an audio file sent via the network connection.

To conduct black-box testing on the Glovo Courier app, we installed it on a specially configured Android mobile phone. In addition to the standard Android functions, we set it up to run additional applications allowing us to analyse the behaviour of the Glovo Courier app. We also configured a computer to be a Wi-Fi access point for that mobile phone. This allowed us to create a virtual environment to analyse the app's code and its communications with the Glovo IT infrastructure.

The first software tool that we used was Mitmproxy, a free tool which helps technical analysts understand which data the app sends and receives. This type of analysis is widely used by research teams studying either a standalone app, or how it is embedded in a more complex framework.[28] With the help of this tool, we were able to intercept all the Internet traffic produced by the mobile phone and to analyse it on our computer. In this way, we were able to analyse the data traffic between the Glovo Courier app and the Glovo platform servers.

We also installed a software tool called Frida which allows developers to work on Android mobile apps from a computer. We conducted a passive form of analysis, meaning that we did not alter the app in any way, but observed how it interacts with the phone, for example when it asks the mobile phone to provide a rider's location (Annex C and D.1).

---

27. See also https://www.eff.org/nb/deeplinks/2022/04/mobile-mitm-intercepting-your-android-app-traffic-go

28. For comparison, see project Data Interception Environment, that packed a toolkit to assist mobile app analysis while looking for privacy leaks https://privacyinternational.org/learn/data-interception-environment, and check out the framework description in https://fadeevab.com/mobile-app-security-testing-tips-notes-ios-android/

Once this setup was ready, we started our observation of the Glovo Courier app through the rider's profile. The app was kept running in the background for 24 hours. This technical setup allowed us to address the research questions related to a rider's location, and whether data was shared with third parties. To address the fourth question, we searched through all the data traffic between the Glovo Courier app and the platform captured by Mitmproxy, looking for any additional elements suggesting the presence of a scoring mechanism.

It is important to note that the type of black-box testing described here is strictly passive. In other words, we did not change or insert any code, or ask the app or platform to execute any tasks, or make it seem as if the rider was performing work-related tasks.

3.4 Results of the black-box testing

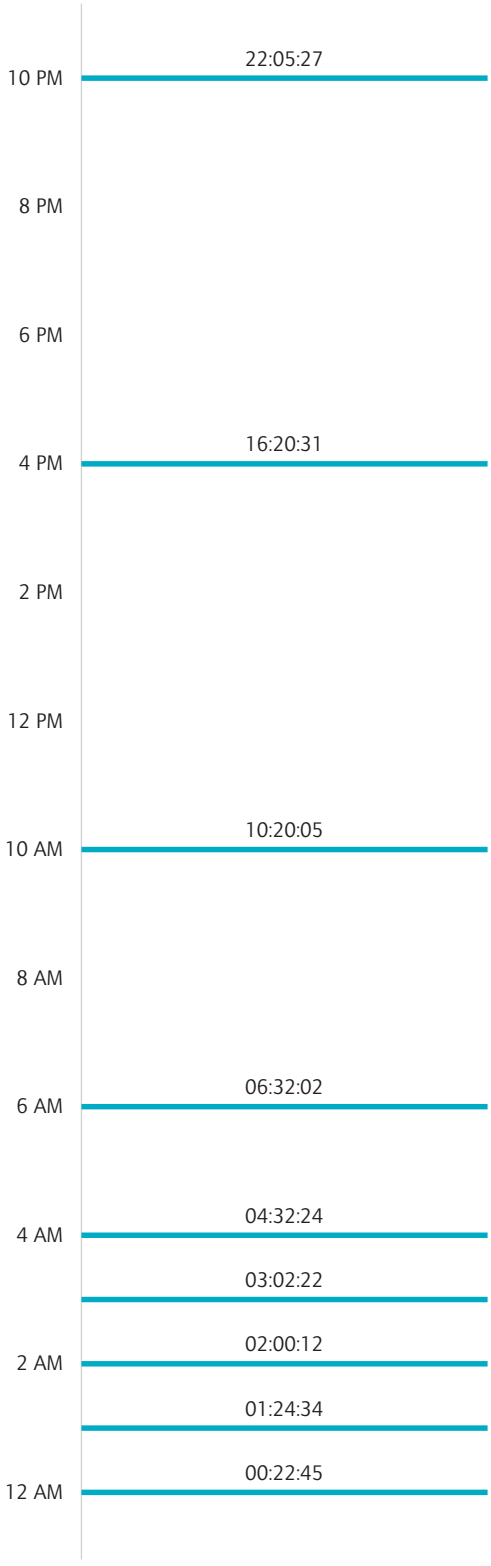
3.4.1 Does the Glovo Courier app track riders' locations outside their working hours?

In the first technical analysis, we found that the Glovo Courier app tracks a rider's location when left running in the background. As an experiment, we left the app running in the background for 24 hours, thus replicating the behaviour of a typical user not logging off properly or closing the app every time.

We requested the Frida tool to report when the Glovo Courier app requests the GPS location of a rider's phone. We found that this happens at rather irregular intervals – for example between 1am and around 3am it requested the location 9 times (01:58:45, 01:58:46, 01:58:49, 01:58:51, 01:58:57, 02:00:12, 02:08:33, 02:09:33, 03:02:22), while it requested it far less frequently during daytime (at 10:20:05, 16:20:31, and 22:05:27).

Repeating the analysis a second time, we found that this behaviour continued to occur, with the Glovo Courier app still querying a rider's GPS location at different times of the day, including outside working hours.

Figure 1 **Location-sharing frequency**



Note: Image generated to visually display the location requests over 24 hours.

3.4.2 What categories of data does the Glovo Courier application share with the platform outside a rider's working hours?

We found out that every time the Glovo Courier app is opened on a rider's phone, even outside working hours, it automatically sent data to the platform, including the exact timestamp of when the information was sent, the exact location of a rider, his speed and his phone's battery level (Annex D.2).

With the help of the Mitmproxy tool, we were able to capture the traffic between the Glovo Courier app and the platform. We divided this traffic into two groups – communication with the Glovo IT infrastructure, and communication with third parties outside the Glovo infrastructure.

With regard to the former, we found out that a rider's location and other data were collected via a specific application interface called Courier Location, part of the Glovo platform designed to receive data from the Courier app. Here is an example of the data sent on 28 July 2021. The timestamp describes the moment when the location was collected, while the other date present in the data payload (start Time) indicates when the app was opened (16 hours earlier).

```
start Time: Wednesday, July 28, 2021 12:15:19.820 AM GMT+02:00,
battery Charging: false,
battery Level: 79,
latitude: 44.4969,
longitude: 11.3515,
speed: 0.0,
timestamp: Wednesday, July 28, 2021 4:20:31.819 PM GMT+02:00
```

We can see that the app sends information on whether the battery is being charged, the battery level, latitude and longitude (location accurate to 10-20 metres) and speed. The data is sent frequently, but irregularly.

We do not know why the app tracks a rider's location at these specific times. We can hypothesise that the intervals depend on the need defined by the platform, for example when there is a high demand for orders and the app wants to check whether there are riders in the area potentially available to fulfil them, even if they did not sign up for a shift. In other words, the Glovo platform has an API dedicated to receiving rider locations and constantly mapping them, regardless of whether they are at work or not.

When an application asks a smartphone (via GPS) where it is, it communicates with the Location service (which merges information from GPS and WiFi networks in the area).

In the second analysis in February 2022, and in the third in July 2022, we observed that the app's behaviour remained the same.

3.4.3 Does the Glovo Courier app share personal data with third parties not mentioned in the privacy policy?

With the help of the Mitmproxy tool, we also analysed all traffic from the Glovo Courier app to third parties outside the Glovo infrastructure. We found evidence of the app sharing data with third parties, including such categories as the GPS location, personal login, name, and a rider's unique identifier. In particular, the data was shared with:

- Pubnub, Kustomer and Smooch – three U.S. companies received the rider's unique user identifier. Analysing the traffic, we deduced that these third-party services were necessary to offer a chat service in the app, though their purpose, as deduced from their product websites, seems broader. As their actual scope is not detailed in the privacy policy, it was impossible for us to determine the exact purpose of the personal data processing.
- Firebase, a Google service intended to help mobile business. Based on Google infrastructure, this product is meant to provide developers with 'a variety of tools and services to help them develop quality apps, grow their user base, and earn profit.' This means that Google may also process the riders' data. It transpired that Firebase received information such as a rider's ID, email address, first name, city code, country code, type of transport used (bicycle, car), version of Android installed on their phone and, what is particularly interesting, their Excellence Score (Annex D.4).
- Braze – a U.S. customer engagement platform used by businesses for multichannel marketing. In the first analysis, we found that Braze received not only a rider's unique ID, but also their email, phone number and location data collected by the platform. The results of the second analysis suggest that the scope of the data share might have been limited to a rider's unique ID (Annex D.5).

We found it particularly problematic that a marketing company should receive such extensive data about the riders, since the data concerns not their customer behaviour but working behaviour. This allows the marketing company to gain an insight into who is working for the company and to use this information for advertising purposes. It contributes to the further blurring of the line dividing consumers and workers, or more broadly between private life and work.

3.4.4 Does the Glovo Courier app perform any additional form of scoring unknown to the rider?

We analysed the contents of the communications between the app and the platform, looking for indications of a scoring, rating or ranking mechanism. We found that the platform's API queried a data field called 'rating'. In the first analysis, we found that the app shared a 'rating' of 4.5 with the platform, although its importance was unclear. (Annex D.3)

The second analysis revealed that this hidden 'rating' was still present. However, a further value was discovered – 'experiment_score' – with a value set to 32.

We have no indication of the purpose of this value, or whether it plays a role in evaluating riders, assigning them orders, or any other automated decision-making process. However, this finding is important, as it demonstrates that traces of automated decision-making can be found through a black-box testing method, helping workers and their representatives formulate further queries about the details of the algorithmic management system.

3.5 Limitations of the mobile app analysis

There are several limitations to the interpretation of our analysis results. Most importantly, black-box testing, even if repeated over time (as in our case), cannot provide conclusive evidence of data protection violations. Such analyses would have to be conducted on multiple riders using the most recent version of the app to yield more extensive evidence that would then have to be evaluated by a court or DPA in the context of other evidence about the algorithmic management system.

Moreover, while we can assume that the same Glovo Courier app is used in other countries where the company operates, black-box testing would have to be conducted with riders from other countries to verify this hypothesis. This kind of analysis would be particularly valuable in the context of Glovo's operations in non-EU countries to verify whether it affects the company's compliance with data protection rules possibly differing from the EU's GDPR rules.

Finally, the Glovo Courier app is updated very frequently, meaning that black-box testing would have to be repeated every time a new update is released in order to check for any changes in the way it collects and processes rider data. A new version of the app is released on average once a week, making it very laborious to analyse every update. We suggest that testing be conducted periodically, for example once or twice a year, to check whether key challenges to data processing persist or have been eliminated.

It is worth noting that the frequent and non-transparent app updates present not only a challenge for the analysts but a risk to the workers themselves. In practice, a piece of code can be introduced at any moment, for example to lock out a single rider or an entire group of riders from being assigned work, with any such change possibly going unnoticed.

To properly assess the app's impact on the protection of rider data, the technical experts would need to have access to the full technical documentation of the algorithmic system. Such an assessment would require an extensive code audit conducted by independent technical experts or in collaboration with the company's experts. As such code audits are very expensive, they are only rarely performed. In our view, they might be necessary when a company refuses to provide sufficient technical documentation of its algorithmic system, in which case the court or DPA could compel/order such to be conducted at the company's expense.

Despite these limitations, we consider black-box testing to be extremely valuable for gaining insights into how mobile apps access, collect and share user data. It is cheap: the tools used are mostly free and require little effort. It is quick: once the tools are known, analysing an app and spotting suspicious evidence can be done in a couple of days. The time required increases when a researcher wants to test more peripheral conditions. Moreover, the method can be easily replicated and adapted to other contexts.

3.6 Discussion of the findings

The technical evidence we collected points to a pervasive data collection system implemented by Glovo. The role of the mobile app is to directly harvest information from riders' phones, including their exact location, the speed at which they are moving and the battery level of their phone, and send it to the platform's servers. Our findings indicate that this data is collected and shared even outside riders' working hours, for as long as the app is left running in the background. Moreover, we found that data was shared directly from the phone with third parties for unknown purposes. We also found some evidence of 'ratings' that might have been automatically assigned to the riders. To sum up, the technical evidence provides insights into the data sent from riders' phones to the platform's algorithmic management system.

The findings can be used as supportive evidence in assessing whether the company complied with the data protection rules set forth in the GDPR. However, we found that the legitimate purpose of the data processing was not clear to riders from the privacy policy, and that processing was performed without sufficient attention paid to riders' privacy, suggesting that it might have been illegal.

As for the question of legitimate purpose, we found that the privacy policy did not offer a clear explanation allowing riders to fully understand what happens to their data once it is harvested from their phones. For example, the purposes indicated therein give the impression that it will only be processed for very specific reasons and within specific timeframes – for example to detect and investigate fraud and criminal offenses, or to manage incidents or claims with insurance companies.

By contrast, our findings indicate that location tracking is conducted continuously and automatically – without verifying the actual need for the processing. The purpose of collecting and processing large amounts of tracking data by the platform, also outside working hours, was unclear. Even more disconcerting were the reasons why the tracking data was shared with third parties, for example marketing companies. We can only speculate that such data is used to map riders' locations at any given time, even outside their working hours, or to compute their performance scores. However, the purpose of such extensive data collection and processing, and potentially automated processing, should be crystal clear to riders.

As for paying due care to a data subject's rights, we found evidence that the extensive data collection and processing were done without regard to several

principles listed in the GDPR, including the principles of data minimisation, of fairness and transparency of data processing and of integrity and confidentiality.

It appears that the Glovo Courier app was not compliant with the principle of data minimisation concerning the scope of the data collected from the riders but, quite the opposite, enabled the platform to continuously monitor riders' locations and behaviour. One simple step to reduce the amount of data would be to disable the location feature when riders are not on shift. However, our evidence demonstrates that the company has little interest in this. We have anecdotal evidence that it actually encourages riders to leave the app running in the background, extending the scope of data collected to their private lives.

The technical evidence also suggests that Glovo's use of the mobile app undermined the principle of fairness and transparency of data processing, since its functioning was not sufficiently explained to riders. To put it simply, riders were unable to understand what the app was doing with their data, therefore not allowing them to adjust their behaviour accordingly – for example to close the app properly, or to demand that tracking be limited to their working hours.

We also found supportive evidence that the principle of integrity and confidentiality was violated. This principle stipulates that a company should refrain from sharing data in an uncontrollable fashion. However, our evidence suggests that Glovo used the mobile app to share data with so many third parties that it could not have reasonably monitored how it was being processed. From the perspective of the data subjects, in this case the riders, it would be virtually impossible for them to exercise their data rights vis-à-vis so many different third parties, should they for example want their data rectified or deleted.

In general, our findings on the role of the Glovo Courier app are consistent with the Italian DPA's findings on the algorithmic management system used by the Glovo platform. We learned from the decision that the platform never submitted a data protection impact assessment (DPIA) to the DPA. To justify this, the platform claimed that it was not necessary, as it did not consider its technology to be of an 'innovative nature'. However, in our view the evidence clearly points to a need for a thorough assessment of the risks to which a data subject is subjected in the context of the company's algorithmic management system. We therefore concur with the DPA's assessment in this regard.

A company is required to perform a DPIA whenever its data processing is likely to result in a high risk to individuals. This is particularly the case when, for example, a company uses systematic and extensive profiling or automated decision-making to make significant decisions about people, as was clearly the case with Glovo. In our opinion, conducting a DPIA would have helped the platform identify the challenges of the Glovo Courier app's design and remove the features creating risks to riders' rights.

In conclusion, we found evidence that Glovo disregarded riders' rights in the design of the Glovo Courier app. We suggest that updates to the app should limit the scope of location tracking to working hours and that the sharing of tracking

or personal data with any third party be stopped. Moreover, riders should be properly informed about the role played by the app in the company's algorithmic management system. This information should include the types of data collected, shared and processed by the platform, whether the processing is done automatically or with human involvement, and what exactly are the parameters used to evaluate a rider's performance and compute internal ratings, such as the Excellence Score. This information should be explicitly mentioned in the company's privacy policy, or other documents made available to riders, preferably before they sign the contract with the company.

In short, the Glovo platform should properly inform riders of the role played by the Glovo Courier app in accessing, collecting and processing their data before they even install it on their private phones.

4. Lessons learned

In this chapter we summarise four lessons learned from the Glovo case that can be applied to other cases involving platform and possibly other work. These lessons show the unique role that technical experts, trade unions, and data protection authorities can play in monitoring and enforcing workers' rights in digitalised workplaces.

4.1 Technical experts can help detect violations of workers' rights

As demonstrated in this study, certain algorithmic management elements can be scrutinised by technical experts even without the knowledge or cooperation of the company concerned. The full architecture of the algorithmic management system is usually concealed from workers and their representatives by platform companies reluctant to reveal how it works even when pressured by authorities. However, by compelling workers to install the mobile app on their private phones, they create a point of entry for technical investigation through a method called 'black-box testing'.

Deploying this method of technical analysis may represent a solution to platform companies' lack of cooperation. Black-box testing provides quick insights into the operations that the app performs on the worker's phone and the types of data communicated to the platform. This means it can help reveal which data is accessed, collected and shared by the app, and the extent to which a worker's behaviour is monitored. This may result in monitoring practices being discovered that workers were previously unaware of, as well as discrepancies with the privacy policy communicated by the company.

Most importantly, this type of analysis can help uncover data privacy and protection violations. For example, it can help reveal whether the app is tracking riders' locations even when they are not working. It can be used to check what other personal data is being harvested from the phone and whether it is transferred directly to third parties, for example marketing companies. The method can also provide insights into the data categories used in automated processing, possibly helping assess the risk of discriminatory outcomes (for example in the case of face recognition technologies). These discoveries can constitute important evidence in assessing whether the platform's app is compliant with a worker's data protection rights under the GDPR.

Compared to other forms of technical analysis, black-box testing does not require many human or technical resources – all that is needed is a technology expert with knowledge of mobile software analysis and the consent of a worker. This type of analysis can be easily repeated to check whether app updates have changed the way workers' data is accessed and shared. Black-box testing can also be easily replicated in the same company operating in a different country, or in other platform companies, paving the way for valuable comparative studies. Finally, this method is not limited to platform companies but can be conducted in any type of workplace that requires workers to install a mobile app on a phone.

However, gaining a full understanding of the inner workings of an algorithmic management system requires a more complex analysis that can only be conducted with the cooperation of the company concerned. Such a full code audit conducted by independent technical experts could be very costly. We suggest that companies failing to provide sufficient information on their algorithmic management to data protection authorities should be compelled to conduct such independent code audits at their expense in the event of potential data privacy violations.

4.2 Data protection authorities can help enforce workers' rights

Data protection authorities can play a vital role in monitoring and enforcing workers' rights by conducting their own investigations into algorithmic management systems. The Italian DPA's investigation of Glovo demonstrated that, although fulfilling that role requires significant resources, national data protection authorities can effectively sanction data protection violations, even in cases requiring cross-border cooperation with their counterparts in other EU countries.

Assessing whether algorithmic management systems violate workers' rights requires high levels of expertise in data protection rules as well as in new technologies and information security. Data protection authorities are uniquely positioned to recruit professionals with such technical expertise, but adequate resources have to be earmarked for this purpose. Concerning enforcement in the employment context, additional resources for cooperation with technical experts and workers' representatives could improve the protection framework for platform and other workers affected by algorithmic management systems.

As demonstrated by the Italian DPA, a national data protection authority does not have to follow up a complaint from a data subject or other player, but can initiate critical investigations *ex officio*. However, by simplifying and promoting complaint procedures, national DPAs can also increase awareness that workers are also data subjects and can play a crucial role in monitoring the use of new technologies in a workplace. DPAs could also provide additional guidance to employers working with algorithmic management systems, for example on how to conduct and submit a data protection impact assessment. In addition to financial penalties for violations of GDPR rules, DPAs could also consider sanctioning

non-compliant companies by obliging them to conduct an independent code audit at their expense.

Finally, the transnational business models of platform companies require DPAs to cooperate across national borders. In a recent case, a number of NGOs from around the EU worked together to file complaints against the advertising industry body, triggering the cross-border cooperation of several national DPAs. This cooperation resulted in a decision to sanction the advertising industry body for insufficient consent procedures. The decision was issued by the Belgian DPA and confirmed by many of its counterparts in other EU Member States.[29] In a similar vein, DPAs could conduct coordinated investigations and issue simultaneous decisions in the case of platforms or other companies operating in multiple countries. The European Data Protection Board could support such efforts with additional guidance.

4.3 Trade unions can use technical expertise to defend workers' rights

This type of analysis can be particularly useful to trade unions – organisations uniquely positioned to defend workers' rights and facilitate cooperation between technical experts and workers. First, trade unions can build connections with technical communities with a view to recruiting experts interested in conducting this type of analysis. Second, they can help identify platform companies where algorithmic management is likely to pose challenges to workers' rights and encourage workers to cooperate in this type of study. Finally, trade unions can help build trust between the parties and ensure that the process is respectful towards workers, for example by providing detailed explanations of how such results will be used and establishing formal consent procedures.

Trade union involvement would allow this method to be replicated among other workers of the same company or in other companies. Trade unions could also support cooperation in cross-border investigations to expose how platform companies operate in different countries. Publishing the results of such studies would create valuable insights for workers, researchers and policymakers and help further our understanding of the use of algorithmic management systems in the platform economy and beyond.

Crucially, trade unions and workers' representatives can use the technical analysis results to defend workers' interests in collective bargaining procedures. They can use the insights on how data is accessed, collected and processed during work to help workers address this aspect in consultations and negotiations with a platform. They can encourage workers to make data protection rules a subject of collective bargaining and ultimately help improve the working conditions of platform workers.

---

29. EDRi, Belgian authority finds IAB Europe's consent pop-ups incompatible with the GDPR, 16.02.2022.

Moreover, trade unions can also turn to national courts and DPAs when a technical analysis reveals that a platform might be infringing data protection rules. Although national procedural laws differ between Member States, trade unions could use the technical evidence to file complaints with national DPAs on behalf of workers. They could also encourage national DPAs to conduct cross-border investigations, with the EDPB assisting and guiding such studies.

In countries where trade unions face challenges in representing platform workers, other players, such as researchers, NGOs or informal workers' collectives, can also play an important role in collecting technical evidence and securing workers' rights. The methods used by these various players might also have to adapt to national contexts – depending on the case, the workers might require the support of collective bargaining initiatives, complaints to data protection authorities, labour inspectorates or other relevant national authorities, strategic litigation in national or supranational courts, campaigns in traditional or social media, or mobilising workers' collective action. We believe that the challenges posed by the use of algorithmic management systems in the workplace can be overcome by engaging the players and methods best suiting the context of a particular country and company.

4.4 Cooperation between technical experts, trade unions and DPAs can improve enforcement of workers' rights

We found that technical analysis can be a catalyst for synergies between the efforts of enforcement agencies on the one hand, and workers' representatives on the other. Closer cooperation between experts and institutions able to understand new technologies and information security, data protection rules and labour laws would strengthen the protection of workers' rights.

Combining top-down and bottom-up efforts in collecting evidence of algorithmic management systems can mutually reinforce workers' rights. Even fragmentary evidence collected directly from workers in bottom-up studies conducted by technical experts can contribute to a wider understanding of developments in the working conditions of platform workers and inspire other players, including workers, trade unions and public authorities, to conduct more in-depth investigations. Conversely, top-down institutional actions, like a coordinated study into platform companies, can also create a favourable environment for workers, researchers and other players to collect further evidence, pool and compare it, and draw new conclusions.

As for the enforcement of data protection rules in an employment context, the diversity of national labour law systems and procedural rules continues to pose a challenge. However, this diversity also creates an opportunity to test different models of cooperation between players. In countries with stronger collective bargaining laws and institutions, trade unions can play a leading role in promoting and enforcing workers' rights in algorithmic management systems.

In other countries, this important role can be played by national courts, data protection agencies and civil society organisations, for example digital rights NGOs. Combining institutional resources for collecting and sharing evidence can help address the information asymmetry created by the platform economy and improve the working conditions of platform and other workers.

Conclusions

Concluding this report, we reflect on the future of workers' rights in the context of steps that can be taken by technical experts, DPAs and trade unions. We also situate our reflections in the broader context of debates about solutions best able to address the challenges ahead of workers.

We hope that technical experts can benefit from access to the full technical documentation of our mobile app analysis. We submitted the technical evidence on the Glovo Courier app to the Italian DPA to demonstrate the potential of black-box testing and support further investigations. We hope to disseminate this report among communities of technical experts to inspire them to engage in similar projects with workers and their representatives. Ultimately, our goal is to lower the entry barrier for research so that workers' rights and privacy experts can scrutinise applications deployed in smaller regions or companies.

We also have high hopes for the growing role of DPAs in enforcing workers' rights across EU. The Italian DPA's decision is likely to have a positive impact on platform workers across the EU. To start with, when Glovo updates its algorithmic management system to comply with the decision, workers in other countries will benefit. Furthermore, the Italian DPA could share its expertise with other DPAs, while cross-border cooperation between different agencies can advance enforcement of the GDPR in an employment context. Finally, high financial penalties, as seen in the Glovo case, can send an important warning to platforms and other companies operating in the EU that disrespect of workers' (human) rights can seriously dent their profits.

We see trade unions as the natural partner of workers in protecting and accessing their rights in digitalised workplaces. We hope to see them taking an active role in collecting evidence of how workers' data is accessed, collected and processed in an employment context and in sharing it with researchers and policymakers to help identify persisting and emerging challenges related to the use of new technologies. We also hope that they can use their power to test new advocacy models best fitting the diverse national contexts. We also hope that new legislative initiatives can strengthen their role in defining the rules governing technology at work.

In our opinion, the current GDPR legislative framework has proven to be both robust and flexible. However, there are still many challenges to the enforcement of the framework that need to be resolved in order to help workers and other data subjects access their rights.

First, enforcement of Art. 22 GDPR is still in its early stages, with few courts having decided to sanction companies for non-compliance with this provision in an employment context or other spheres of life.[30] Understanding how Art. 22 is implemented requires analysing the legal reasoning behind the decisions where a court has ruled in favour of workers, as well as those where the platform has successfully argued that it does not rely on automated decision-making, as seen in the Uber case in the Amsterdam District Court.[31] Second, the 'flexibility clause' of Art. 88 GDPR creates an uneven playing field for EU workers who have to rely on diverse national labour laws and collective agreements to access their rights. In particular, in countries where collective bargaining rules are weaker or absent, workers have fewer possibilities to negotiate how new technologies are used in the workplace. Finally, as they pointed out in a recent contribution, civil society organisations recommend addressing enforcement challenges by harmonising national procedures for the application of data protection rules, by boosting the resources available to DPAs and the EDPB, performing joint investigations and coordinating their action through taskforces.[32] These recommendations also apply to the enforcement of GDPR in an employment context.

The introduction of automated decision-making in a growing number of workplaces might also require consideration of innovative solutions going beyond the existing legislative framework. These solutions might involve new legislative proposals to strengthen workers' rights, such as the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work submitted by the European Commission in December 2021.[33] Interestingly, Article 9 (3) of the draft proposal included a provision that the platform workers' representatives or the platform workers concerned may be assisted by an expert of their choice, in so far as this is necessary for them to examine the matter that is the subject of information and consultation, and to formulate an opinion. The costs of this expertise would be covered by the platform if it has more than 500 workers in a Member State. If adopted, the Directive would apply only to platform workers, but hopefully also pave the way for other legislation advancing the rights of other types of workers affected by algorithmic management.

Moreover, we might have to rethink the legislative framework, putting greater emphasis on collective data governance in the workplace. As one scholar put it, 'digital workspace transformations require negotiation and bargaining between workers and management to proceed, and therefore must be collectively governed rather than only individual consented' (Moore, 2021:25). Designing and

---

30. An overview of the case law is available at https://gdprhub.eu/index.php?title=Category:Article_22_GDPR

31. Rechtbank Amsterdam (2021), Zaaknummer C/13/687315 / HA RK 20-207, 11.03.21. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020

32. EDRi, Civil society call and recommendations for concrete solutions to GDPR enforcement shortcomings, 16.03.2022. https://edri.org/our-work/civil-society-call-and-recommendations-for-concrete-solutions-to-gdpr-enforcement-shortcomings/

33. European Commission (2021) Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final, 09.12.2021.

institutionalising collective data governance in the workplace is one of the most pressing human rights puzzles for civil society and policymakers alike.

Thinking outside legislative frameworks, we can also imagine that platform accountability be addressed by innovative technical means. This would require reversing the current logic where the automated profiling of workers takes place in a split of a second, while accessing human rights might take months. Innovative technical solutions could offer real-time accountability instruments as opposed to lengthy data subject procedures or litigation in courts. Platform companies who care about workers' needs and rights should replace existing systems with new ones where workers, trade unions and data protection experts participate in their design.

Ultimately, the use of algorithmic management systems has exacerbated the existing power imbalance between workers and their employers. Addressing this imbalance and safeguarding workers' rights will require concerted efforts from researchers, public institutions, trade unions and policymakers alike, and most importantly from workers themselves.

References

Ajunwa I. (2018) Algorithms at work: productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law, SSRN Scholarly Paper 3247286, Social Science Research Network. https://papers.ssrn.com/abstract=3247286

Ajunwa I. (2020) The paradox of automation as anti-bias intervention, Cardozo Law Review, 41 (5), 1671–1742.

Aloisi A. and De Stefano V. (2020) Delivering employment rights to platform workers, Il Mulino, 31.01.2020. https://www.rivistailmulino.it/a/delivering-employment-rights-to-platform-workers

Aloisi A. and De Stefano V. (2021) 'Frankly, my rider, I don't give a damn', Il Mulino, 07.01.2021. https://www.rivistailmulino.it/news/newsitem/index/Item/News:NEWS_ITEM:5480

Anderson D.N. (2016) Wheels in the head: ridesharing as monitored performance, Surveillance & Society, 14 (2), 240–258. https://doi.org/10.24908/ss.v14i2.6018

Ball K. (2010) Workplace surveillance: an overview, Labor History, 51 (1), 87–106. https://doi.org/10.1080/00236561003654776

Barocas S. and Selbst A.D. (2016) Big data's disparate impact, SSRN Scholarly Paper 2477899, Social Science Research Network. https://doi.org/10.2139/ssrn.2477899

Bernhardt A., Kresge L. and Suleiman R. (2021) Data and algorithms at work: the case for worker technology rights, UC Berkeley Labor Center.

Bronowicka J. and Ivanova M. (2021) Resisting the algorithmic boss: guessing, gaming, reframing and contesting rules in app-based management, in Moore P. and Woodcock J. (eds.) Augmented exploitation: artificial intelligence, automation and work, Pluto Press.

Chan N.K. and Humphreys L. (2018) Mediatization of social space and the case of uber drivers, Media and Communication, 6 (2), 29–38. https://doi.org/10.17645/mac.v6i2.1316

De Stefano V. et al. (2021) Platform work and the employment relationship, Working Paper 27, ILO.

Edwards L. and Veale M. (2017) Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for, LawArXiv. https://doi.org/10.31228/osf.io/97upg

Gillespie T. (2014) The relevance of algorithms, in Gillespie T., Boczkowski P.J. and Foot K.A. (eds.) Media technologies: essays on communication, materiality, and society, The MIT Press. https://doi.org/10.7551/mitpress/9780262525374.003.0009

Grandi G.Z. and Pettinelli R. (2020) A 50 anni dallo statuto: 'l'art. 4 è morto. viva l'art. 4!', Lavoro Diritti Europa, 2.

Ivanova M. et al. (2018) The app as a boss? Control and autonomy in application-based management, Europa-Universität Viadrina. https://doi.org/10.11584/arbeit-grenze-fluss.2

Kellogg K.C., Valentine M.A. and Christin A. (2020) Algorithms at work: the new contested terrain of control, Academy of Management Annals, 14 (1), 366–410. https://doi.org/10.5465/annals.2018.0174

Kocher E. (2022) Digital work platforms at the interface of labour law: regulating market organisers, Hart Publishing.

Kroll J. et al. (2017) Accountable algorithms, University of Pennsylvania Law Review, 165 (3), 633-705.

Moehlmann M. and Zalmanson L. (2017) Hands on the wheel: navigating algorithmic management and Uber drivers' autonomy, in ICIS 2017 Proceedings. https://aisel.aisnet.org/icis2017/DigitalPlatforms/Presentations/3/

Moore P. (2021) AI trainers: who is the smart worker today?, in Moore P. and Woodcock J. (eds.) Augmented exploitation: artificial intelligence, automation and work, Pluto Press, 13-29.

Parodi E. (2021) Milan prosecutors order food delivery groups to hire riders, pay 733 million euros in fines, Reuters, 24.02.2021. https://www.reuters.com/business/milan-prosecutors-order-food-delivery-groups-hire-riders-pay-733-mln-euros-fines-2021-02-24/

Prassl J. and Risak M. (2015) Uber, Taskrabbit, and co.: platforms as employers? Rethinking the legal analysis of crowdwork, Comparative Labor Law & Policy Journal, (3), 619-652.

Safak C. and Farrar J. (2021) Managed by bots: data driven exploitation in the gig economy, Worker Info Exchange. https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_8d720d54443543e2a928267d354acd90.pdf

Soro A. (2019) La nuova emergenza per la privacy mondiale si chiama app economy, Garante per la protezione dei dati personali. https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9074044

Thompson P. (2003) Fantasy island: a labour process critique of the 'age of surveillance', Surveillance & Society, 1 (2), 138–151. https://doi.org/10.24908/ss.v1i2.3350

Vallebona A. (2020) L'incertezza del diritto del lavoro, Massimario di Giurisprudenza del Lavoro, 4, 1067-1074.

Wagner B. (2019) Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems: human agency in decision-making systems, Policy & Internet, 11 (1), 104–122. https://doi.org/10.1002/poi3.198

Zuboff S. (2019) The age of surveillance capitalism: the fight for the future at the new frontier of power, Profile Books.

All links were checked on 30.06.2023.

Annexes

Annex A – Questionnaire

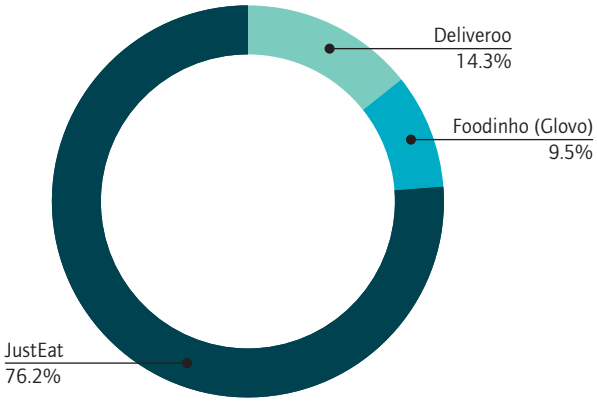
Context: The team at the Tracking Exposed project wanted to recruit couriers who could help this study about worker's rights by providing the credentials to access their app. For this purpose, we designed a questionnaire to identify their situation.

Note: The questionnaire that follows has been written with an Italian audience in mind, therefore there are some references (q.5) to Italian national employment options, and the q.1 references companies that have operated in Italy.

A.1 In which food delivery company do you work (or have you worked)?

- Foodinho (Glovo)
- JustEat
- Deliveroo
- UberEats
- Gorillas
- Mymenu
- Wolt
- DeliveryHero (Foodora)

Figure 2 **Answers from 21 participants**



Note: For context, one of the primary contacts was the internal representative of a JustEat worker union, and this might have affected the amount of contributions received from the riders there.

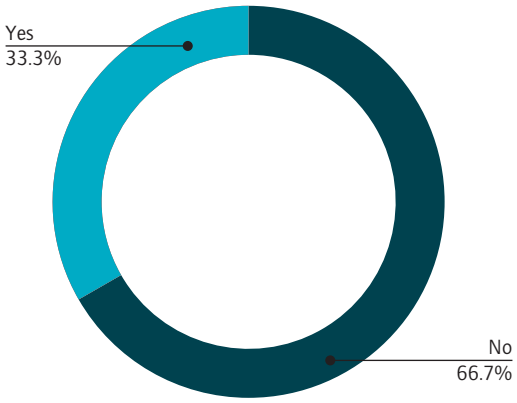
Source: The Tracking Exposed + IRPI questionnaire results.

A.2 How did you get hired?

Options	Answers
Through a job interview	2 (9.5%)
I have submitted an online application	19 (90.5%)
I simply use an account	

A.3 Have you had an in-person interview with someone belonging to the company you applied for?

Figure 3 Onboarding process experiences



Note: A total of 21 participants in 2022.

Source: The Tracking Exposed + IRPI questionnaire results.

A.4 Have you signed a contract to work?

Options	Answers
Yes	21 (100%)
No	

A.5 What kind of contract have you signed?

Options	Answers
The so-called "Collaborazione occasionale"	2 (9.5%)
A fixed term contract (tempo determinato)	4 (19%)
You are an autonomous worker (P.IVA)	3 (14.3%))
I haven't signed a contract	
A permanent contract (tempo indeterminato)	12 (57.1%)

A.6 If you are an autonomous worker (P.Iva or similar), how do you organize your daily work? If there are problems during the work, is there a dialogue with the company?

Free text answer:

- I have 15 hours of contact but I have to work 5 days a week. The assignments shift outside shift planning without my consent. I asked for a minimum 4h shift but sometimes they give less. Some orders are too far away (5-8 km) even though I work with a regular bicycle.
- I go to work only when I want it.

A.7 What application do you use to work?

Options	Answers
The official app provided by the delivery platform	21 (100%)
An unofficial app provided by others	
I'm using a device that doesn't belong to me	
I don't use an app	

A.8 What information did you receive from the company regarding the job app?

Options	Answers
The platform has given you directions on how to use it	14 (66.7%)
You have learned to use the app on your own	6 (28.6%)
None of the above	1 (4.8%)

A.9 Are you the owner of the account you use to work with?

Options	Answers
Yes	20 (95.2%)
No	1 (4.8%)

A.10 To your knowledge, has anyone verified if your account really belongs to you?

Options	Answers
No, it was never verified by anyone	3 (14.3%)
Yes, they have verified my identity through an online authentication procedure	6 (28.6%)
Yes, they verified my identity through an in-person check	7 (33.3%)
I don't know	5 (23.8%)

A.11 Have you ever encountered one or more of these events during the delivery job?

Because the answer to A.11 supports one or more of the options, a percentage is not reported.

- Your work account has been suspended (*3 riders*).
- Your work account has been closed (*0 riders*).
- Your shift has been canceled (*7 riders*).
- Did you felt penalized by the system (*11 riders*).
- They didn't give you assistance when you contacted the platform (*15 riders*).

- You have received an incorrect Feedback or evaluation against you (*4 riders*).
- You have received penalties that have resulted in your inability to access work (*5 riders*).
- No (*4 riders*).

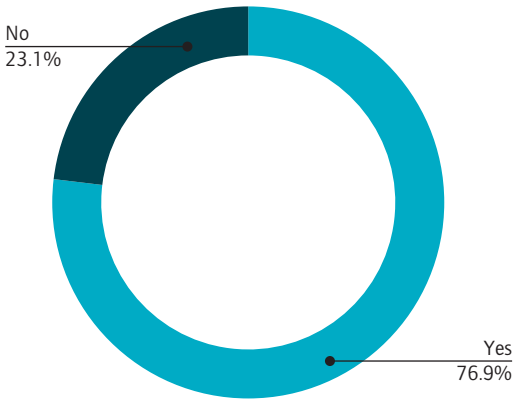
A.12 What significant effects did these events have on your work or personal life?

Because the answer to A.12 supports one or more of the options, a percentage is not reported.

- I haven't been able to work for a while (*2 riders*).
- I suffered a penalty from the company (*0 riders*).
- I felt excluded and not helped (*11 riders*).
- I thought about changing job (*7 riders*).
- None of the above (*4 riders*).
- Other (*2 riders*).
- I have never encountered any problems while working, so I haven't any significant effect on my daily life (*2 riders*).

A.13 In case you have suffered a sanction from the company, have you been informed?

Figure 4 **Sanctions and transparency**



Note: To this question 13 riders answered.

Source: The Tracking Exposed + IRPI questionnaire results.

A.14 Have you tried to contest the sanction that was given to you? If so, how?

Free text answer:

- I tried by following the procedure available.
- I display evidences.
- I updated my coordinates and provided the necessary evidences.

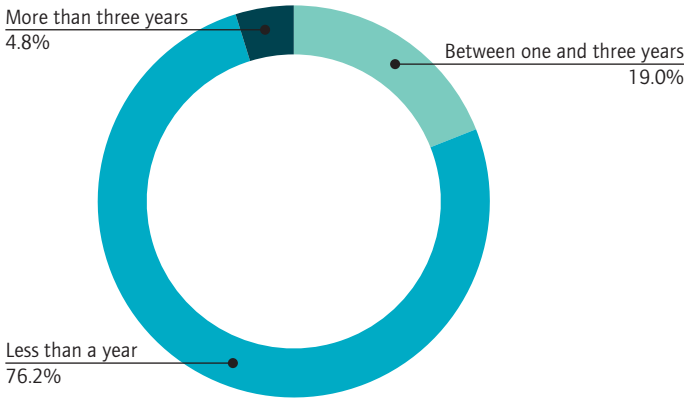
A.15 Has the company responded to your dispute?

answer to A.14	Result
I tried by following the procedure available	Responded
I display evidences	Not responded
I updated my coordinated and provided the necessary evidences	Responded

A.16 How long have you been working for the delivery platform?

- Less than a year.
- Between one and three years.
- More than three years.
- I've worked in the platform it in the past.

Figure 5 How long they have worked



Note: Zero riders answered "I've worked in the platform it in the past".

Source: The Tracking Exposed + IRPI questionnaire results.

A.17 To successfully organize possible collective lawsuits against digital platforms that violate workers' rights, we may need your help. If you are interested leave us your email.

This question was functional to our investigation, to further develop technical analysis with the riders that want to offer their time to collaborate in the technical analysis, as it is important to include active workers.

Annex B – Technical terminology and the analysis tools used

Below is a detailed description of some of the terms and tools referred to in the report.

In our research, we used the first three techniques listed below, with the fourth considered for potential advancement.

Table B1 **Four methods used in mobile app studies**

System call hooking, or passive behaviour analysis	When an application has permission to access a dedicated portion of the device, it has to issue a specific function call implemented by the operating system (Android, in this case) to actually access the data. We temporarily modified the Android system to report when an application asks for that information by hooking this call. While not actually tampering the application under scrutiny, this allows us to check whether our operating system is being interrogated in a sensitive area. https://frida.re/docs/home/
Traffic analysis	This is the process of intercepting and examining messages to observe information from communication patterns; it is also possible to perform this within encrypted connections like the one directed to HTTPS services, as long as you have physical access to the device allowing you to install a Certification Authority under the analyst's control https://docs.mitmproxy.org/stable/concepts-certificates/
Code instrumentation	This technique is a method of automated interface testing; a developer might instruct a tool to act as if someone else was working. The method facilitates test repeatability. However, as it is a limit of the test, it also implies that we would only have a portion of code reachable from the interface. https://en.wikipedia.org/wiki/Instrumentation_(computer_programming)
Real case research	More than a technical enhancement, this is a methodology advancement. It requires that the analyst uses the app in the same way as a courier, performing deliveries, rejecting orders, etc. Performing actions measured by the platform assigns additional meanings to the information collected with the technical mechanisms described above.

To carry out this research, we used both manual tests and professional tools. Specifically, the software used was as follows:

1. **JADX**, an open-source tool to decompile Java code from an Android application; This tool is useful for opening .apk (Android Package) files and dissecting the app between code and other resources. The Java code is converted into a readable format, providing a (rough) understanding of how the app behaves. The tool cannot decompile everything, and decompiled code is notoriously not very readable. Nonetheless, it is a good starting point for understanding an app. https://github.com/skylot/jadx
2. **JEB**, a professional proprietary tool to decompile and analyse Android applications. https://www.pnfsoftware.com/jeb/manual/android/
3. **Frida**, a free software framework allowing you to "inject your own scripts into black box processes. Hook any function, spy on crypto APIs or trace private application code, no source code needed. Edit, hit save, and instantly see the results". One of the most powerful tools for use in observing how an application behaves, it might also be deployed in a mobile phone belonging to a participating worker. In this context we focused on the use of a Frida-server installed on the test phone to

modify the behaviour and functionality of the Android operating system as seen by the application. https://frida.re/

4. **MitmProxy**, an open-source application used to intercept HTTP/HTTPS traffic generated by the application in question. It allows the data traffic between app and platform to be saved, thus understanding which information is passing through. Unfortunately, we never know what is stored on the platform's servers, though it is not wrong to assume that everything sent is also recorded indefinitely for business, surveillance, and worker profiling purposes. https://mitmproxy.org/

Annex C – The code injected via Frida

Frida allows code to be injected into the Java Virtual Machine. In practice, a researcher can thus change an app's behaviour.

However, these changes can be divided into two categories: "active" and "passive" ones:

- **Active** occurs when the analyst wants to change am app's workflow. We did not use this functionality in our study. Our goal was to keep the company accountable, and not to distort their intent.
- **Passive** is when an analyst decides not to interfere with the expected behaviour of the app. Instead, as in this case study, he simply adds code to makes visible what is happening (for instance, functions that print or detail logging mechanisms).

The code is released as part of this report because, by doing so, we might help trade unions, their consultants, and other researchers to replicate the analysis.

(location.js) This code is licensed as AGPL-3 (c) by Gaetano Priori

```
function getLoggingDateAsString() {
  return new Date().toString();
}
var  f  =  new  File("/data/data/com.glovoapp.courier/files/logger.
txt", "w");

Java.perform(function () {
  const Location = Java.use("android.location.Location");

  var location = Location.$new("gps");

            Location.$init.overload("android.location.Location").
implementation =
    function (x) {
      console.log("Instantiated new location ( Location ) ");
      return location;
    };

    Location.$init.overload("java.lang.String").implementation  =
function (x) {
    console.log("Instantiated new location ( String ) ");
    return location;
  };

  Location.getLatitude.implementation = function () {
    console.log(
      "com.glovoapp.courier fetched Latitude : " +
        this.getLatitude() +
        " at: " +
```

```
        getLoggingDateAsString() +
        "\n"
    );
  };

  Location.getLongitude.implementation = function () {
    console.log(
      "com.glovoapp.courier fetched longitude : " +
        this.getLongitude() +
        " at: " +
        getLoggingDateAsString() +
        "\n"
    );
  };
  // The following function bypass the "fake location check" if
is used.
  Location.isFromMockProvider.implementation = function () {
    console.log("Location.isFromMockProvider -> false");
    return false;
  };
});
```

The portion of code that matters in this analysis is the block starting with Location.getLongitude.implementation and the one Location.getLatitude.implementation because it simply injects our piece of code into Glovo Courier app, allowing us to print a line to the terminal any time the app ask for a GPS location.

Annex D - Technical evidence

In this annex we list five different pieces of technical evidence. They have been initially collected in July 2021, and then confirmed by repeating the tests in February 2022 and September 2022.

The first analysis was on the app version 2.92.0, the second on version 2.120.0, and the third on version 2.146.0.

Based on our consistent observations of recurring behaviors, it can be reasonably concluded that the issues highlighted here are not temporary, they are long-term operational practices within Glovo.

D.1 Evidence from Glovo analysed using Frida

As explained above, the code within the Glovo app was modified, with the aim of reporting how often the app accesses the device's GPS. When this happens, it prints a line to the terminal with the date and the latitude and longitude value, so that the analyst can keep track of it.

Please note that this test concerns the first analysis, in July 2021. When repeated in September 2022, we have found an increased frequency of GPS accesses.

Below is a portion of these printouts (July 2021):

```
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 00:22:45 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 00:22:45 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:24:34 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:24:34 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:45 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:45 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:46 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:46 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:46 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:46 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:49 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:49 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:51 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:51 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:57 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:57 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 02:00:12 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 02:00:12 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 02:08:33 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 02:08:33 GMT+0200
```

```
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 02:09:33 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 02:09:33 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 03:02:22 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 03:02:22 GMT+0200
com.glovoapp.courier fetched Latitude : 45.4969 at: Wed Jul 28 2021 04:32:24 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 04:32:24 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 06:32:02 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 06:32:02 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 10:20:05 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 10:20:05 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 16:20:31 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 16:20:31 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 22:05:27 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 22:05:27 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 22:05:27 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 22:05:27 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 22:06:27 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 22:06:27 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 22:09:32 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 22:09:32 GMT+0200
```

Below is a portion from the printouts (September 2022):

```
com.glovoapp.courier fetched Latitude : 44.497357085552612 at: Tue Sep 06 2022 09:35:06 GMT+0000
com.glovoapp.courier fetched longitude : 11.353691612824080 at: Tue Sep 06 2022 09:35:06 GMT+0000
com.glovoapp.courier fetched Latitude : 44.49740884555261 at: Tue Sep 06 2022 09:35:19 GMT+0000
com.glovoapp.courier fetched longitude : 11.35343624371289 at: Tue Sep 06 2022 09:35:19 GMT+0000
com.glovoapp.courier fetched Latitude : 44.497714607168204 at: Tue Sep 06 2022 09:35:25 GMT+0000
com.glovoapp.courier fetched longitude : 11.35326917487001 at: Tue Sep 06 2022 09:35:25 GMT+0000
com.glovoapp.courier fetched Latitude : 44.497764354711214 at: Tue Sep 06 2022 09:36:06 GMT+0000
com.glovoapp.courier fetched longitude : 11.35300832409896 at: Tue Sep 06 2022 09:36:06 GMT+0000
com.glovoapp.courier fetched Latitude : 44.49814915462392 at: Tue Sep 06 2022 09:37:06 GMT+0000
com.glovoapp.courier fetched longitude : 11.35294021753365 at: Tue Sep 06 2022 09:37:06 GMT+0000
com.glovoapp.courier fetched Latitude : 44.498499910231075 at: Tue Sep 06 2022 09:38:06 GMT+0000
com.glovoapp.courier fetched longitude : 11.352830500947344 at: Tue Sep 06 2022 09:38:06 GMT+0000
com.glovoapp.courier fetched Latitude : 44.49896315494858 at: Tue Sep 06 2022 09:39:06 GMT+0000
com.glovoapp.courier fetched longitude : 11.352527306436857 at: Tue Sep 06 2022 09:39:06 GMT+0000
com.glovoapp.courier fetched Latitude : 44.49901944802352 at: Tue Sep 06 2022 09:40:06 GMT+0000
com.glovoapp.courier fetched longitude : 11.35231336305463 at: Tue Sep 06 2022 09:40:06 GMT+0000
```

(The full evidence would have been three page long and has been reduced for simplicity.)

D.2 Traffic intercepted between the app and the platform

The information here reveals nothing unexpected as, in the privacy policy signed by the rider, it is explained that the platform processes information such as the rider's location. This processing purpose is in line with the service provided.

But we want to add a further consideration. In the report below you can see one of the many connections from the phone to the Glovo infrastructure, reporting the device's geolocation.

```
2021-07-28 16:20:32 POST https://api.glovoapp.com/v3/courier/
position HTTP/2.0
                          ← 200 application/json 2b 155ms

{
    "accuracy": 14.599,
    "activities": [
        {
            "confidence": 0,
            "start_time": 1627424119820,
            "type": "UNKNOWN"
        }
    ],
    "batteryCharging": false,
    "batteryLevel": 79,
    "latitude": 44.4969,
    "longitude": 11.3515,
    "reactionType": "TIME_OUT",
    "speed": 0.0,
    "timestamp": 1627482031819
}
```

We see two numbers reported (start_time and timestamp). They look like what is called a UNIX timestamp (the number of seconds since the 1st of January 1970). It is a standard way to transmit dates in digital communication.

We want to draw your attention to two values:

variable name	deducted meaning	value
start_time	when the Glovo Courier app was opened for execution	1627424119820
timestamp	the moment when the information was reported to the platform	1627482031819

Converting them give us:

variable name	value	converted
start_time	1627424119820	Tue Jul 27 10:15:19 PM CEST 2021
timestamp	1627482031819	Wed Jul 28 02:20:31 PM CEST 2021

These details fit our experiment's parameters.

We conclude from the mere presence of this data that:

1. The Glovo platform knows when the rider opened the app, and that this information is sent every time (start_time is present every time the location is sent).
2. the app incessantly reports the rider's location even if the rider has not been working for 16 hours (this was our test case, the app started at 10 PM, while the timestamp of this last recording reads 2PM on the following day.

The current implementation does not seem in line with the principle of data minimisation, as it actually leads to logging where workers are located, even if they have forgotten to turn off the app, as it remains running in the background.

Two conditions could have been used to automatically assume the rider isn't working: the lack of movement (the GPS location has been the same during all the test) and the not active participation to any delivery task. Opinion of the authors is that one of these condition should have been sufficient for the app to stop revealing the worker's GPS location.

D.3 Intercepted data revealing a "hidden scoring"

In Glovo, there are two official types of score, the one assigned to restaurants (https://blog.glovoapp.com/en/glovo-score/) and the one charting the reliability of delivery workers in accepting orders (https://delivery.glovoapp.com/gh/faq/excellence-score).

Analysing the traffic, we detected an unexpected, additional "rating" with the value of 4.5; below is the block of data passing between the app and the platform servers (we have removed the rider's personal data).

We have no knowledge of how or whether this data, as well as other data present in these transmission logs, is used, as it is one of the limits of reverse engineering.

But considering rating is often associated with a form of worker discrimination, its mere presence might be a reason for a trade union to ask the company to ensure there are not additional and undisclosed ratings that might affect the workers.

```
2021-07-27 23:59:15 PUT https://api.glovoapp.com/v3/users/
glv:courier:8b5acd06-b0b2-44f1-a203-⊖REDACTED❞- HTTP/2.0

{
   "NIF": "-⊖REDACTED❞FISCAL-CODE--",
   "autoAssignentEnabled": true,
   "cityCode": "BOL",
   "deleted": false,
   "deliveredOrdersCount": 0,
   "description": null,
   "deviceUrn": null,
   "email": "-⊖REDACTED❞-@gmail.com ",
   "enabled": true,
   "forceNewPassword": false,
   "id": -⊖REDACTED❞ID--,
   "locale": "en_US",
   "mcc": true,
   "mediaCampaign": null,
   "mediaSource": null,
   "name": "-⊖REDACTED❞NAME--",
   "phoneNumber": {
       "countryCode": "IT",
       "number": "+39-⊖REDACTED❞PHONE-"
   },
  "picture": "ProfilePhotos/-⊖REDACTED❞NAME--_-⊖REDACTED❞ID--",
   "preferredLanguage": "en",
   "preferredLanguageRegion": "US",
   "rating": 4.5,
   "sourceCompany": null,
   "sourceCompanyOrders": null,
   "transport": "BICYCLE",
   "type": "Courier",
   "urn": "glv:courier:8b5acd06-b0b2-44f1-a203--⊖REDACTED❞-"
}
```


D.4 Google and the analysis of third-party services

Most modern applications communicate with more than one infrastructure. Each of those contacted could potentially process personal data.

For this reason, a privacy policy must indicate which third parties process data, whereby these third-party platforms are called data processors under the GDPR.

It is important to check whether each platform contacted is accurately described in the privacy policy, as is often the case with Google.

Below is an example collected by mitmproxy, in this case capturing traffic to a third party in which it transfers personal data.

It is important for those conducting investigations to check that all third parties processing personal data are mentioned in the privacy policy, as well as the purpose of processing.

Again, you will notice portions of removed data. This is to protect the anonymity of the rider who participated in the study.

```
2021-07-28 00:15:17 POST https://firebaseremoteconfig.googleapis.
com/v1/projects/716238041317/namespaces/firebase:fetch

Accept:          application/json
Content-Length:  880
User-Agent:      Dalvik/2.1.0 (Linux; U; Android 10; Redmi 5 Plus
Build/QQ1B.19⊖REDACTED▪▪.011)
Host:            firebaseremoteconfig.googleapis.com
Connection:      Keep-Alive
Accept-Encoding: gzip

{
    "analyticsUserProperties": {
        "courier_android_version": "29",
        "courier_city_code": "BOL",
        "courier_country_code": "IT",
        "courier_email": "⊖REDACTED▪▪@gmail.com ",
        "courier_excellence_score": "--",
        "courier_id": "⊖REDACTED▪▪",
        "courier_name": "⊖REDACTED▪▪",
        "courier_transport": "BICYCLE"
    },
    "appId": "1:7⊖REDACTED▪▪7:android:25⊖REDACTED▪▪0c",
    "appInstanceId": "eC4⊖REDACTED▪▪li",
    "appInstanceIdToken": "e⊖REDACTED▪▪w",
    "appVersion": "2.95.0",
    "countryCode": "US",
    "languageCode": "en-US",
    "packageName": "com.glovoapp.courier",
    "platformVersion": "29",
    "sdkVersion": "20.0.2",
    "timeZone": "Europe/Rome"
}
```

D.5 Other third-party services

Most modern applications communicate with more than one remote server. This means when a user opens an app, a variety of servers are contacted, whereby each of them may or may not be a legitimate data processor.

We can observe and highlight whether and which personal data is shared with further third-party companies.

Below you can see a dump of the data sent to the infrastructure of braze.eu, this evidence is from our first analysis in July 2021.

```
2021-07-28 01:58:56 POST https://sdk.fra-01.braze.eu/api/v3/data
201 Created application/json
Request Response Detail
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Braze-Api-Key: c0a5c797-f7df-4bba-8c9b-6c9376d1b5c9
Content-Length: 412
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; Redmi 5 Plus Build/
QQ1B.191205.011)
Host: sdk.fra-01.braze.eu
Connection: Keep-Alive

{
  "api_key": "c0a5c797-f7df-4bba-8c9b-6c9376d1b5c9",
  "app_version": "2.95.0",
  "app_version_code": "107830.0.0.0",
  "device_id": "f9-⊖REDACTED❝-da",
  "events": [{
    "data": {
      "altitude": 282.6000061035156,
      "latitude": 44.4969,
      "ll_accuracy": 13.432000160217285,
      "longitude": 11.3515
    },
    "name": "lr",
    "session_id": "f7-⊖REDACTED❝-1e",
    "time": 1627430331.549,
    "user_id": "-⊖REDACTED❝-"
  }],
  "sdk_version": "6.0.0",
  "time": 1627430335
}
```

The redacted userID was expressed as a number. As it is the same information we also found in D.3 (API with Glovo platform), we can safely assume it is a privacy leak of personal data uniquely tied to an actual worker.

The GPS coordinates, as well as an altitude and an accuracy estimation, are also present.

These information were sent to the third party outside of any working shift.

Braze is a "Customer Engagement Platform" (quoting their website "Power customer-centric interactions between consumers and brands in real-time"). Operating under the domain name braze.eu, each third party service, as a processor of personal data, should be explicitly mentioned in the Privacy Statement, and offered as an opt-in.

Moreover, trade unions can, in their collective bargaining procedures, hold companies accountable for sharing workers' data with undisclosed third-party companies.

The following example shows traffic with the same company, Braze, and was recorded in our last analysis, on September 2022.

```
POST /api/v3/data HTTP/2
Host: sdk.fra-01.braze.eu
X-Braze-Triggersrequest: true
X-Braze-Datarequest: true
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Braze-Api-Key: c0a5c797-f7df-4bba-8c9b-6c9376d1b5c9
Content-Length: 5684
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Google Pixel
Build/OPR6.170623.017)
Connection: Keep-Alive

{
  "device_id": "e6f-⊖REDACTED❝-e8f8",
  "time": 1662385143,
  "api_key": "c0a5c797-f7df-4bba-8c9b-6c9376d1b5c9",
  "sdk_version": "15.0.0",
  "app_version": "2.146.0",
  "app_version_code": "123910.0.0.0",
  "device": {
    "os_version": "26",
    "carrier": "Android",
    "model": "Samsung Galaxy S4",
    "resolution": "1080x1794",
    "locale": "en_US",
    "remote_notification_enabled": true,
    "android_is_background_restricted": false,
    "time_zone": "GMT"
  },
  "attributes": [
    {
      "user_id": "-⊖REDACTED❝-",
      "email": "-⊖REDACTED❝-@gmail.com",
      "phone": "+39-⊖REDACTED❝-",
      "push_token": "cBspy52_S6KLKfuWwCD_rP:AP[...]Ju"
    }
```

```
  ],
  "events": [
    {
      "name": "lr",
      "data": {
        "latitude": 44.49708739691707,
        "longitude": 11.35118673961445,
        "altitude": 0,
        "ll_accuracy": 0
      },
      "time": 1662384163.619,
      "user_id": "-⊖REDACTED▪▪-"
    },
    {
      "name": "ss",
      "data": {},
      "time": 1662384105.341,
      "user_id": "-⊖REDACTED▪▪-",
      "session_id": "38804621-⊖REDACTED▪▪-12b229ef3e"
    },
    {
      "name": "se",
      "data": {
        "d": 892
      },
      "time": 1662384058.305,
      "user_id": "-⊖REDACTED▪▪-",
      "session_id": "ceb66cfa-⊖REDACTED▪▪-de99d6406e"
    },
    { [...] }
  ],
  "respond_with": {
    "user_id": "-⊖REDACTED▪▪-",
    "triggers": true,
    "config": {
      "config_time": 1660-⊖REDACTED▪▪-
    }
  }
}
```


The userId personal data (redacted), as well as the rider location, was still sent to the Braze server.

The format of the communication has a new structure, and again the data payload has been redacted for protect the identity the rider. Because the data would have been four pages long and the content of the events variable is not easily understandable, it was more practical summarize here its composition.

The list was originally composed of 14 events type ”lr”, 8 type “ss” and 10 of type “se”. The meaning of the events type lr, also because contains the GPS coordinates, can be estimated to be a “location request” message. The meaning of the other types, ss and se, is unknown to us.

In total these 32 events describes the activity of the riders happened in a time span of 27 minutes.

Also in this case, the third party service was receiving the information outside of any working shift.

Annex E - Glovo Courier App Privacy Policy

Below are portions of the Glovo Courier App Privacy Policy that focus on the sections describing sharing data with third parties and geolocation data. The original source was retrieved in May 2022 from the URL https://glovoapp.com/en/legal/privacy-couriers/. It appears to have been last amended in December 2019.

3.1 Data Processed

a) Information supplied directly by Users:

- *Registration Data*: the information provided by Users when they create an account on the GLOVO Platform: username and e-mail.
- *User Profile Information*: the information added by Users on the Platform in order to be able to use the GLOVO service; i.e. their mobile phone number and delivery address. Users can view and edit the personal data on their profile whenever they wish. GLOVO does not store Users' credit card details, but these are provided to licensed electronic payment service providers, who receive the data included directly and store it in order to facilitate the payment process for Users and to manage it on GLOVO's behalf. This information is under no circumstances stored on GLOVO's servers. Users may delete the details of the credit cards linked to their account at any time. This will trigger the service provider to delete the information, which will have to be re-entered or selected in order to place new orders through the Platform. Users may request such providers' privacy policies at any time.
- *Additional information that Users wish to share*: any information that a User could supply to GLOVO for other purposes. Examples include a photograph of the User or the billing address in the case of Users who have asked to receive invoices from GLOVO.
- *Information about previous communications with GLOVO*: GLOVO will have access to the information supplied by Users for the resolution of any queries or complaints about the use of the platform, whether through the contact form, by e-mail or by phone through the customer service.
- Information on accidents involving any of the parties involved in the provision of services through the Platform for the purpose of making insurance claims or carrying out any other actions with the insurance companies contracted by GLOVO.
- Transcription and recording of conversations held between the USER and GLOVO for the processing of incidents, queries or any other consultations that may be made.
- *Information on Communications between Users and Mandataries*: GLOVO will have access to the communications exchanged between Users and the Mandatories that collaborate with the Platform by means of the chat system provided on the Platform.

b) Information indirectly supplied by Users:

- *Data arising from the Use of the Platform*: GLOVO collects the data arising from Users' Use of the Platform every time they interact with the Platform.
- *Data on the application and the device*: GLOVO stores data on the device and the Application used by Users to access the services. This data is:
  - The IP address used by each User to connect to the Internet using his/her computer or mobile phone.
  - Information about his/her computer or mobile phone, such as his/her Internet connection, browser type, version and operating system, and type of device.
  - The full uniform resource locator (URL) Clickstream, including date and time.

- *Data from the User's account*: information on the orders made by each User, as well as feedback and/or comments made about them by such User.
  - The User's browsing history and preferences.
- *Data arising from the User's origin*: if a User arrives at the GLOVO Platform through an external source (such as a link from another website or a social network), GLOVO collects data on the source from which the GLOVO User arrived.
- *Data resulting from the management of incidents*: if a User contacts the GLOVO Platform through the Contact Form or on GLOVO's phone number, GLOVO will collect the messages received in the format used by the User and may use and store them to manage current or future incidents.
- *Data arising from "cookies"*: GLOVO uses its own and third-party cookies to facilitate browsing by its users and for statistical purposes (see the Cookie Policy).
- *Data resulting from external third parties*: GLOVO may collect personal data or information from external third parties only if the User authorises such third parties to share that information with GLOVO. For example, if a User creates an account through their Facebook account, Facebook could disclose to us the personal data of that User that can be found on his/her Facebook profile (such as name, gender or age).

  Similarly, if a user accesses GLOVO through products and services offered by Google, Google may send the User's browsing data to GLOVO, with access to the platform through the links created by Google.

  The information provided by the external third party may be controlled by the User in accordance with the third party's own privacy policy.
- *Geolocation Data*: provided that this has been authorised by Users, GLOVO will collect data relating to their location, including the real-time geographic location of their computer or mobile device.

Annex F - Technical considerations and assessments of analysis strategies

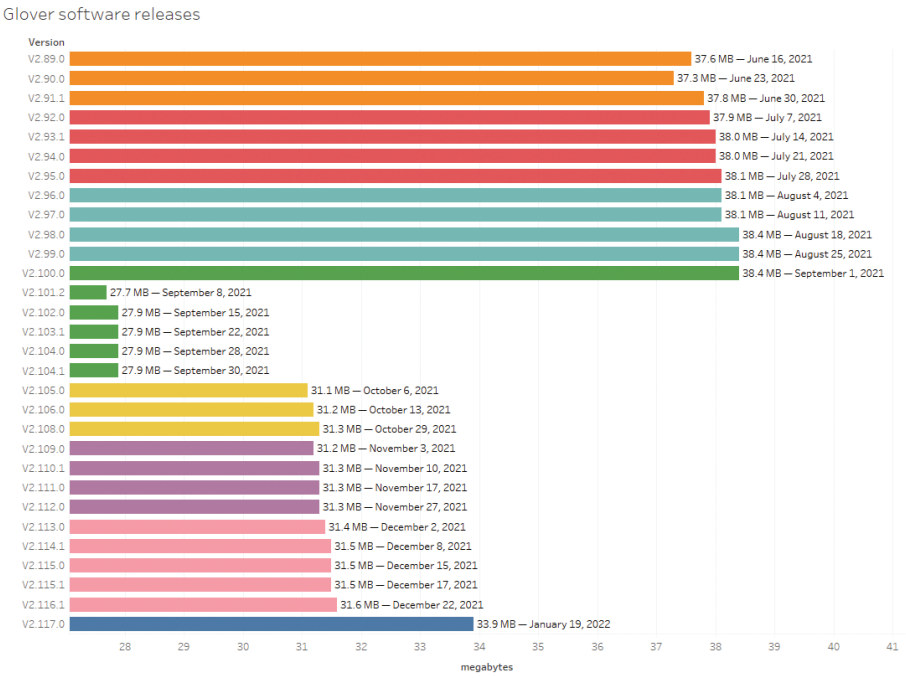
The gig ecosystem is characterised by frequent releases of new versions, updates and fixes. The release procedures are usually so automated that a new software version can be made available by developers with just a few clicks.

Unless explicitly disabled, the new version then automatically updates the worker's cell phone. But how often do such updates occur?

We created the image below from the freely available information on https://apkpure.com/glovo-courier/com.glovoapp.courier/versions, a website tracking the updates of a given mobile application published on the Android marketplace.

In the chart, the text reports the version number and the date on which the version was published. Each colour represents a month, thereby highlighting how many updates occur on average, while the length of the lines represents the size of the app. The chart represents only 30 updates (between June 2021 and January 2022).

Figure 6 **Application Size by Release**



Note: Bar size represents the size in Megabyte.

Source: Image generated to visually display 30 updates of the Glovo courier app.

Variations in the size of the app do not always imply a big change in its code. Technical explanations might exist: for example, the addition of a new multimedia resource, or the compression of existing resources that could have been optimised in the first place. A small change might mean code updates from previous versions.

For example, many technical reasons may also justify the decrease in size seen between version 2.100.0 on 1 September and the next one on 8 September, as well as the increase between December and January. Even if we can't make assumptions about the meaning of the update, we want to focus on how Glovo (and any other app developer) has the possibility to arbitrarily release an update, force this update to be downloaded, and install new code on a worker's device. This can invalidate past analyses like the one reported in this paper, by eliminating the problematic behaviour, or can make it harder for analysts like ourselves to inspect it.

We need to consider that each of our analyses took two weeks of work. If a new app version is released weekly or bi-weekly, it implies that any report produced would soon be outdated, making it difficult to hold a company to account.

In the time window reported above, Glovo was fined by the Italian DPA. One of the remedies stated was to issue new, updated versions, with new safeguards in place. Considering the release frequency, it is not always possible to infer when such updates occur. In the case of companies turning out releases less often, or with a more visible CHANGELOG file, it would have been possible to know when the remedies were deployed in the Google Play Story.

European
Trade Union Institute
etui@etui.org
www.etui.org

D/2023/10.574/27
ISBN: 978-2-87452-689-3 (print version)
ISBN: 978-2-87452-690-9 (electronic version)

etui.