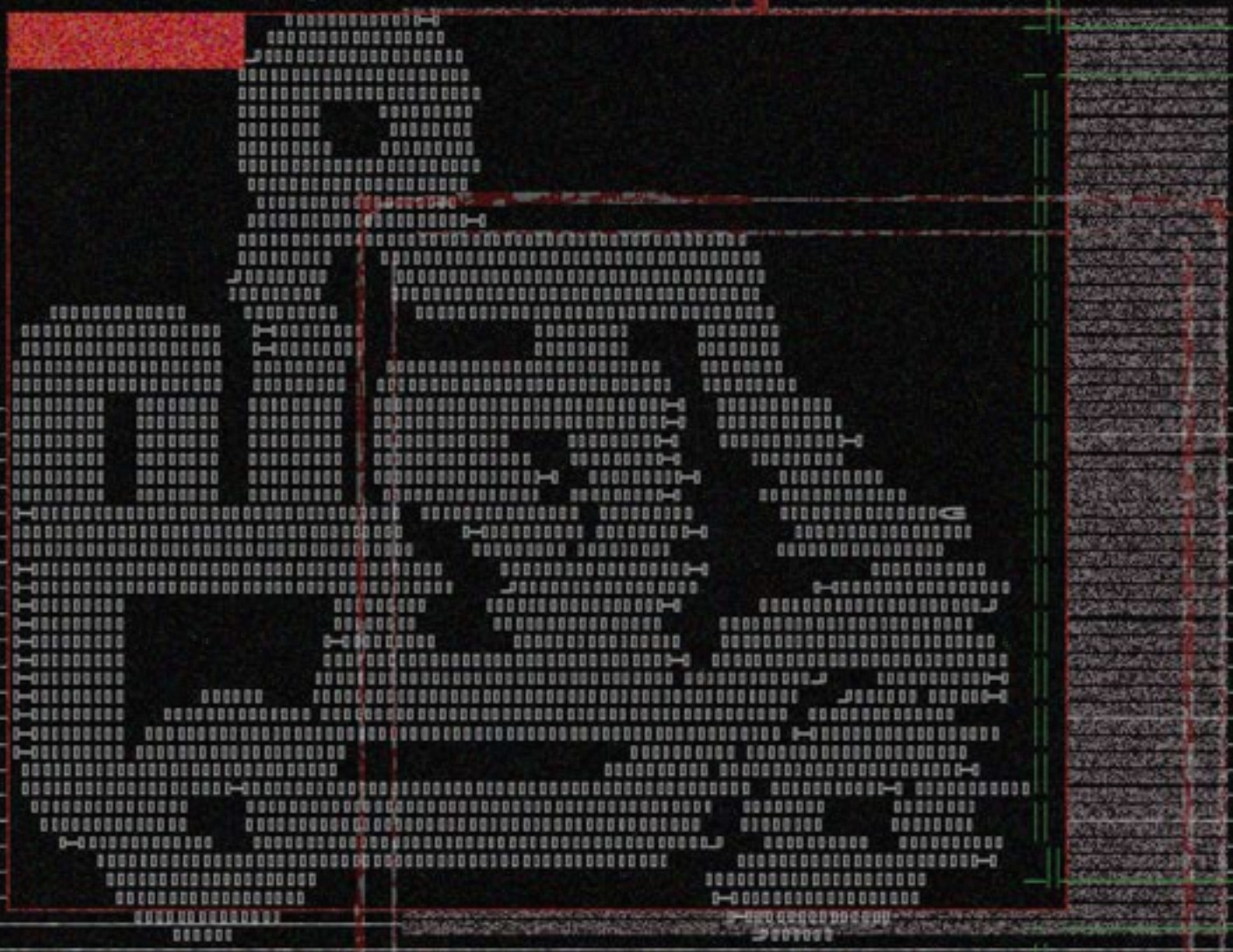
Reversing the Gaze

How to Study Workplace Apps and Reclaim Worker's Rights

Reversing.Works


```
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",
```

Reversing the Gaze

How to Study Workplace Apps and Reclaim Worker's Rights

Reversing.Works
https://reversing.works/

Simone Robutti
Claudio Agosti
Joanna Bronowicka
Gaetano Priori

Handbook design and editorial support
Daniela Vaccaro

Publication Date: September 2026
Funding **European Artificial Intelligence & Society Fund**

INDEX

1. INTRODUCTION

You are a food delivery worker, and the app assigning your orders continuously tracks your location.

You are a taxi driver, but if you refuse a ride, your rating drops, and future work becomes scarce.

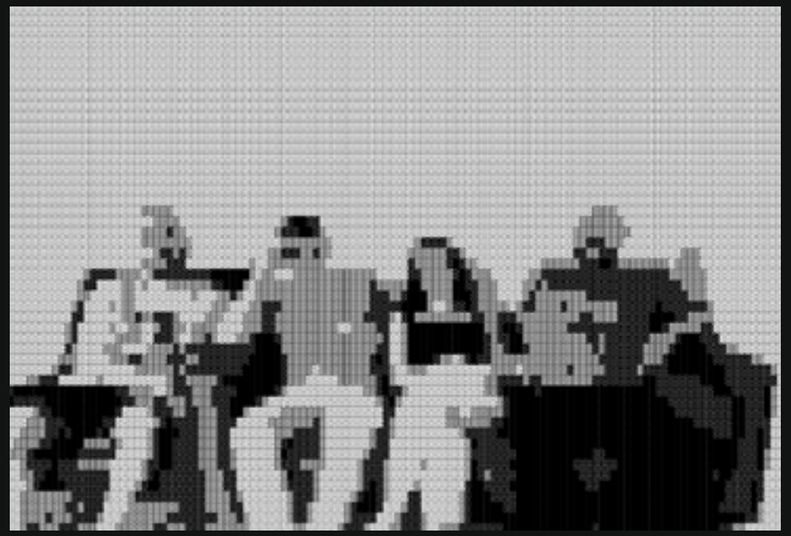
You are a data worker, and the platform you rely on shares your personal data with social media companies.

You are an office employee, yet you must check in via an app on your private phone to start your workday or request leave.

1.1 The challenge: algorithmic management at work

Across a growing number of professions, mobile applications and digital systems are no longer optional: they are a condition of access to work. While often associated with the gig economy, where platforms mediate tasks such as delivery, ride-hailing, or online freelancing, these practices now extend far beyond it. Similar forms of digital oversight are spreading into more traditional sectors, from logistics to to office-based work.

At the core of this shift is the rise of algorithmic management: systems that allocate tasks, monitor performance, and discipline workers through continuous data collection and automated decision-making. While promising efficiency and lower costs, they also reshape the employment relationship by concentrating information in the hands of employers or platforms, creating significant imbalances of power.



1.2 Who we are

We are Reversing.Works, a transdisciplinary research team working to expose and challenge algorithmic management in the digital workplace.

Since 2021, we have developed technical tools that help workers and their representatives identify, document, and challenge algorithmic management practices. By examining the apps and software installed on workers' private devices, these tools generate concrete evidence of how data is collected, processed, and shared.

This evidence is meant to be used. It can support collective action, strategic litigation, and regulatory enforcement, turning opaque technical systems into sites of accountability.

Our work is grounded in ongoing collaboration with a global network of trade unions, NGOs, and digital rights advocates. Together, we translate technical findings into practical strategies for protecting worker rights. Our aim is simple: to help workers regain access to the information used to manage them, and, in doing so, to rebalance power in the digital workplace.

1.3 How we do it

Our work starts from a simple question: how can workers find out what companies know and decide about them?

We answer this by analysing how workplace apps behave in practice; specifically, the data they transmit from a worker's private device to company servers. **This approach** — which we call **network forensics — focuses on real-world data flows to document how information is collected, processed, and shared**, including with third parties, without relying on internal access to company systems.

This approach is lightweight and replicable, yet it has delivered concrete results. Our 2020 investigation into Glovo in Italy, for example, contributed to a landmark decision by the Italian Data Protection Authority, resulting in sanctions of over €7.6 million for unlawful data processing and background tracking.

Our work is anchored in the GDPR, which applies not only to consumers but also to workplace data. It gives workers enforceable rights such as access, transparency, and limits on automated decision-making, which remain underused in practice. We see data protection authorities as key actors in enforcing these rights, particularly where labour protections are weak or absent.

By **equipping workers** and their representatives **with technical evidence,** we aim to support complaints, strengthen accountability, and clarify how the law applies in practice, both to challenge harmful practices and to guide those seeking to do better.

GLOVO/FOODINHO CASE (ITALY)

The Glovo/Foodinho case is a landmark investigation into algorithmic management in platform work involving Glovo (Spain) and its Italian subsidiary Foodinho.

INVESTIGATION

The Italian Data Protection Authority (DPA) launched an ex officio investigation and conducted an unannounced inspection of Foodinho's offices and platform. It found that riders' personal data was accessible across all countries of operation, beyond what was necessary for delivery work.

The DPA requested documentation on algorithms for order allocation and performance scoring, but the information provided was incomplete and inconsistent. Independent technical evidence from researchers, who later formed Reversing.Works, supported the investigation.

DECISION (ORDER NO. 234)

In November 2020, the DPA found breaches of GDPR and Italian labour rules on worker monitoring. In June 2021, it imposed a €2.6 million fine and ordered corrective measures. A further €5 million fine followed in 2024, reinforcing rules on automated decision-making at work.

SIGNIFICANCE

The case shows how regulators, technical experts, and independent research can jointly expose and regulate "black box" algorithmic management in platform work.

How can workers find out what companies know and decide about them?

1.4 Who is this handbook for

This guide is intended for anyone interested in understanding or conducting investigations into digital workplace practices, whether independently or in collaboration with us.

It may be particularly useful if you are:

- **A gig economy worker** seeking to better understand your rights and how to defend them
- **Part of a workers' collective** looking for tools and allies to investigate company practices
- **A union representative or organiser** wanting to understand how data and surveillance shape working conditions
- **An NGO or advocate** working on digital or labour rights
- **A researcher or technically skilled activist** interested in contributing to workplace transparency

1.5 Why this handbook

This handbook was written to open up our work and to make it usable. Over the past years, we have developed and applied a methodology for investigating how workplace technologies operate in practice. Again and again, we encountered the same challenge: many workers, unions, and advocates sense that something is wrong, but lack the tools to prove it. This guide is intended to bridge that gap.

At its core, the handbook is a practical introduction to digital workplace investigations. It explains how to examine the behaviour of apps and systems, how to turn technical observations into evidence, and how that evidence can be used to support action. More broadly, it serves three goals.

- **First, to make digital investigations a common tool** within the labour movement. By sharing our methods, we aim to enable others to carry out their own inquiries and to contribute to a growing network of practitioners.
- **Second, to show how evidence can shift power.** Investigations are often the first step in challenging unfair workplace practices. They transform individual experiences and suspicions into verifiable facts, helping to reduce information asymmetries, support legal complaints, and strengthen advocacy or media work.
- **Third, to foster collaboration** between technical experts and those working on labour and legal issues. Addressing algorithmic management requires combining different forms of expertise. This handbook is an invitation to build those connections and work together on concrete cases.

Starting an investigation
is not just about finding answers.
It is about creating
the conditions to act on them.

1.6 Why start an investigation

If you want to challenge unfair data collection and algorithmic management at work, start an investigation.

Whether you are a worker, a union representative, or an advocate, the first step is the same: gather evidence. Evidence is power. It turns suspicions into facts and lived experiences into proof. It breaks the information advantage companies rely on, and it opens the door to action: complaints, media exposure, strategic litigation, and enforcement.

This is where the GDPR becomes a tool, not just a framework. It applies to workplace data and gives you rights: to access your data, to understand automated decisions, and to challenge unlawful practices.

Investigations often start with a personal question: What is happening to my data? But they rarely stay personal. They reveal patterns, expose systems, and contribute to collective struggles for fairer working conditions. So why start?

TO RECLAIM ACCESS AND BREAK OPACITY

Access to data and decision-making is the real battleground. Companies build technical and organisational barriers to keep workers in the dark. This is not accidental: it is how control is maintained. Investigations push back. They make hidden processes visible and reclaim access to the information that shapes your work

TO BUILD POWER AND DEMAND FAIR CONDITIONS

When you expose how data is collected and decisions are made, you shift the balance of power. What was invisible becomes contestable. What was individual becomes collective. Data protection stops being a personal data issue and becomes a labour issue.

TO USE GDPR AS A TOOL FOR ACCOUNTABILITY

These rights exist: use them. Investigations generate the proof needed to file complaints, engage data protection authorities, and force companies to answer for their practices. This is how the law becomes real.

TO BUILD ALLIANCES THAT CAN WIN

Investigations are not done alone. They bring together workers, unions, technical experts, and legal practitioners. These alliances turn isolated concerns into coordinated action and make challenges harder to ignore.

GDPR CORE PRINCIPLES

The GDPR protects workers' personal data whenever their employer processes information that can identify them. It does not apply to anonymous data, company-only information, or purely private activities outside work.

Employers must follow these key principles:

LAWFUL BASIS

Data must be processed on a valid legal ground (e.g., contract, legal obligation, legitimate interests). In an employment relationship, consent is usually not valid due to the power imbalance between employer and employee!

TRANSPARENCY

You must be clearly informed about how and why your data is used.

STORAGE LIMITATION

Data must not be kept longer than necessary.

SECURITY

Data must be protected against unauthorised or unlawful use.

Data must be protected against unauthorised or unlawful use.

DATA MINIMISATION

Only data that is necessary for the purpose may be collected.

ACCOUNTABILITY

Employers must be able to demonstrate compliance.

ACCURACY

Data must be kept correct and up to date where needed.

GDPR RIGHTS AND REMEDIES

A WORKER HAS THE RIGHT TO:

- ↘ **Be informed**: Know how personal data is used and why
- ↘ **Access data:** Request a copy and details of processing (usually within one month)
- ↘ **Correct data:** Fix inaccurate or incomplete information
- ↘ **Delete data:** Request erasure in specific situation
- ↘ **Restrict use:** Limit how datais processed in defined cases
- ↘ **Object:** Challenge processing based on legitimate or public interest grounds
- ↘ **Automated decisions:** Be protected from decisions made solely by automated systems with significant effects

If these rights are not respected, a worker may:

1. **Complain** to a data protection authority (DPA)
2. **Go to court** for an effective legal remedy
3. **Claim compensation** for material or non-material damage

2. CONDUCTING A REVERSING.WORKS INVESTIGATION

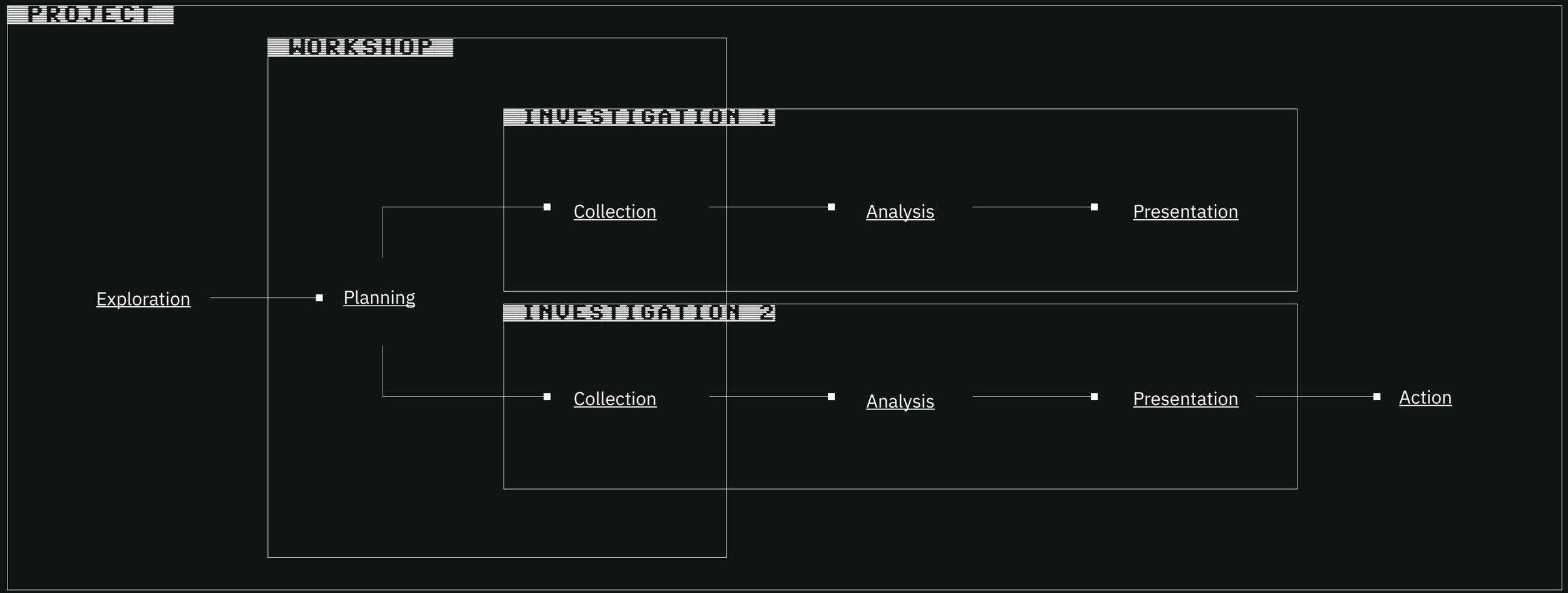
Conducting a Reversing.Works Investigation

This section introduces an investigative approach that has developed through a series of projects and collaborations between 2021 and 2026. It builds on earlier work, including the 2020 investigation into the Glovo courier app in Italy, and has been refined through joint efforts with trade unions, NGOs, researchers, and worker-led organisations. What is presented here is not a fixed methodology, but a synthesis of what has proven useful across different contexts.

Collaboration has been central to this process. Investigations typically bring together complementary forms of knowledge: technical expertise on the one hand, and contextual insight, trust, and access to workers on the other. Partners often contribute a deep understanding of working conditions and relationships with workers, while the technical team develops tools and methods for analysing the technology.

By setting out this approach, we aim to make elements of the process more accessible. It is intended to support further collaborations, but also to be adapted or extended by others. Rather than prescribing a single model, we offer a set of practices that may serve as starting points.

This infographic outlines the phases and activities that structure a Reversing.Works project. Each is described briefly below and explored in greater depth in the sections



EXPLORATION

The starting point of any project. Together with partners, we assess the viability of the investigation, define its scope, identify which apps to focus on, and agree on the resources and effort to invest. This phase also involves mapping potential paths to action once findings are available

WORKSHOP

A structured session conducted with workers to collect data. During the planning phase, it is worth considering whether one or more workshops are necessary, or whether the investigation can be conducted remotely or independently. Where workshops are used, a single session can cover multiple investigations running in parallel, with the same or different workers.

INVESTIGATION

The process of collecting, analysing, and reporting on a single app. Each investigation involves at least one experiment — a data collection session with an individual worker — and may involve several, each with a different worker. Some investigations will yield clear evidence; others will not.

ACTION

Depending on what an investigation finds, follow-up actions may include legal complaints, media engagement, or organising efforts. These may be carried out jointly with Reversing.Works or independently by partners.

2.1 Exploration
What can be revealed?

Exploration → Planning

→

An investigation typically begins with a shared understanding of what this approach can and cannot reveal. As project partners, it is useful to align early on the scope of the method and the kinds of questions it is best suited to address.

At its core, the approach focuses on analysing a workplace app or software installed on a worker’s personal device. The aim is to document what data is accessed, collected, and processed by the company, both during and outside working hours.

From this starting point, investigations are often guided by a small set of recurring questions that help structure the inquiry.

WHAT DATA IS COLLECTED BY THE APP?

Objective:
Identify what data is collected, both actively provided by workers and gathered automatically.

What to look for:
↘ Basic profile data (e.g., identifiers, name, vehicle type),
↘ Operational data (e.g., order histories, earnings, activity logs);
↘ Background data collection (e.g,. location or device data beyond active use)

Indicative findings:
In some cases, investigations have suggested forms of location tracking that extend beyond working hours.

WHAT DATA IS SHARED WITH THIRD PARTIES?

Objective:
Map how data flows to external entities and consider whether the data collected is necessary for performing work.

What to look for:
↘ Data sent to analytics providers;
↘ Marketing or attribution services;
↘ Security and fraud prevention tools;
↘ Other external integrations.

Indicative findings:
Past investigations have pointed to the sharing of detailed data, including location or customer data, with third-party services.

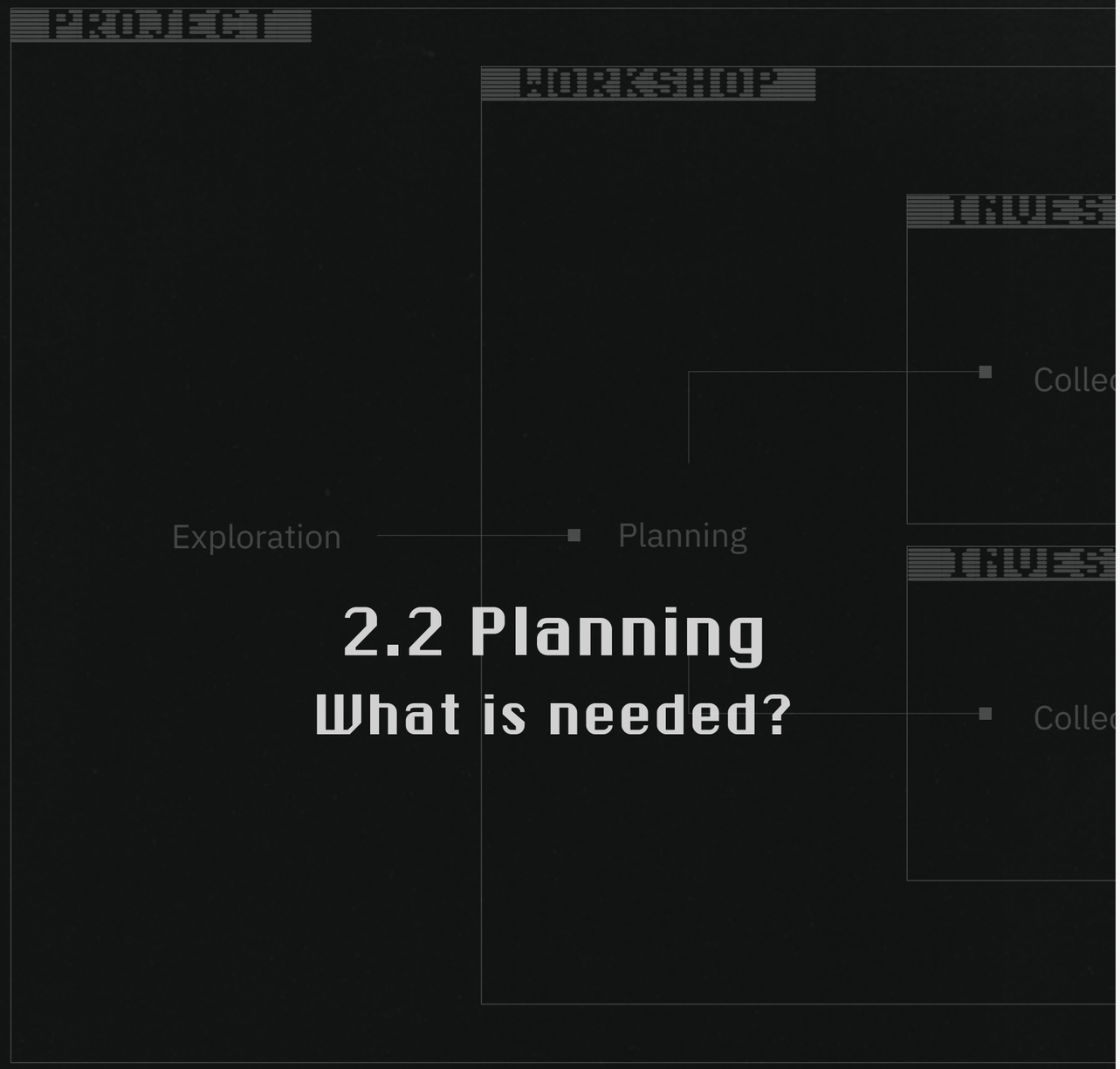
ARE THERE TRACES OF AUTOMATED DECISION-MAKING?

Objective:
Identify technical signals that may indicate profiling or real-time categorisation of workers.

What to look for:
↘ Variables or metrics linked to performance, demand, or behaviour; Indicators of scoring, ranking, or segmentation;
↘ Location-based signals (e.g., zone activity or demand levels)

Indicative findings:
Some analyses have revealed internal variables suggesting dynamic assessment of workers or geographic areas.

Taken together, these lines of inquiry help make certain aspects of platform management more visible. While they do not provide a complete picture, they can support a more informed understanding of how data is used in practice, and contribute to efforts to address information asymmetries between platforms and workers.



→
Once there is a shared interest in pursuing an investigation, the next step is to assess whether the basic conditions are in place. These conditions help ensure that the process is both legally sound and technically feasible. If they are met, it becomes possible to decide what type of investigation is most appropriate for the specific context.

STEP 1

CONFIRM IF WORKERS USE THE APP OR SOFTWARE ON THEIR PRIVATE DEVICES

REQUIREMENT

The target app must be installed on workers' personal devices. Investigations cannot be conducted on company-issued phones or computers for legal reasons.

MOBILE APPS

- The app should be available via the Google Play Store (Android only)
- A preliminary technical check is typically carried out to identify potential security protections or barriers.

COMPUTER-BASED WORK

- Access to the relevant platform (e.g., URL) is required.
- These environments are often somewhat easier to assess and usually do not require the same level of pre-testing.

STEP 2

VERIFY IF WORKERS ARE WILLING TO SHARE LOGIN CREDENTIALS

REQUIREMENT

At least one worker needs to provide access to their account.

GUIDELINES

Participation must be based on informed consent. Workers should clearly understand:

- How the investigation works
- What data may be collected
- Any potential risks involved

ROLE OF PARTNERS

This step is typically facilitated through trusted intermediaries, such as trade unions, NGOs, or worker collectives, who have established relationships with workers.

STEP 3 PICK AN INVESTIGATION FORMAT

Once the basic conditions are in place and trust has been established, the next step is to organise the data collection. In practice, this can take different forms depending on the context, resources, and level of involvement from partners and workers.

Based on our experience, three main formats have emerged. These are not mutually exclusive and can be combined or adapted as needed. The choice of format will depend on the specific context and goals of the collaboration.

1. REMOTE INVESTIGATIONS

When in-person meetings are not feasible, remote investigations offer a more flexible option, though they require careful coordination.

PROS
↘ Reduced travel time
↘ Suitable for longer, more detailed investigations

CONS
↘ Less direct observation
↘ Harder debug/error management
↘ Relies on existing trust and clear communication

2. IN-PERSON WORKSHOP

In-person workshops bring together the technical team, partners, and workers in the same location. They are often effective for collaborative interpretation and hands-on observation. Detailed guidance is provided in the Workshop Guide, but a typical structure includes:

Set-up and introduction [~1 hour]
↘ Preparing devices, explaining the method, confirming consent

Group session [~1 hour per app]
↘ Login and navigation by the worker
↘ Data collection (screen recording and network traffic)
↘ Initial review and discussion

Wrap-up [~30 minutes]
↘ Summarising findings and next steps

PROS
↘ Enables group sessions with multiple workers
↘ Allows direct observation of app use
↘ Helps avoid location-based anomalies

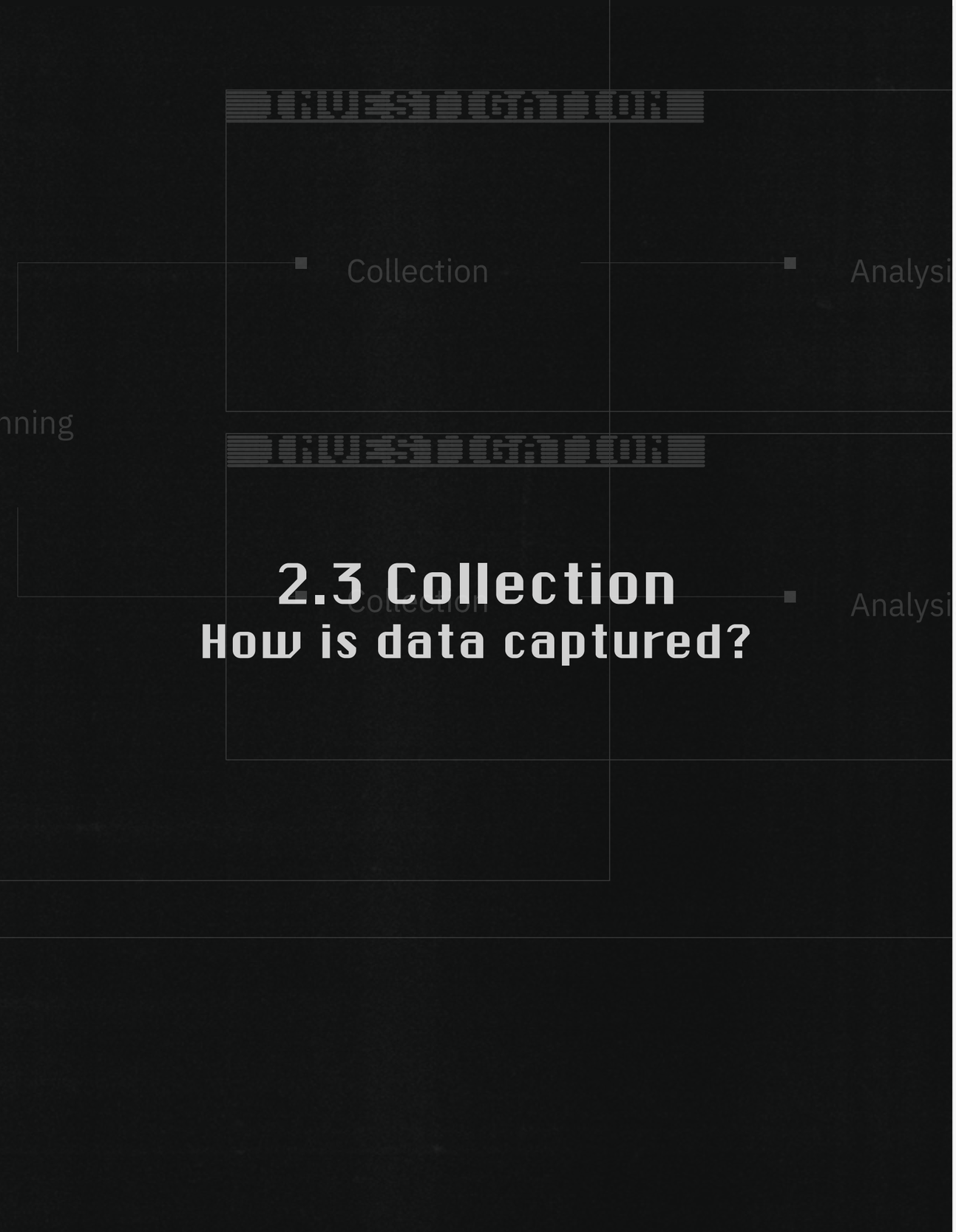
CONS
↘ Time constraints may limit depth
↘ Technical issues can delay the process

3. INDEPENDENT INVESTIGATIONS

Partners or other actors may also carry out investigations independently using shared tools and approaches

PROS
↘ Greater flexibility and autonomy
↘ Can be adapted to local contexts

CONS
↘ May not capture the full depth of a facilitated investigation



2.3 Collection
How is data captured?

→
Our approach to data collection is based on observing live data flows generated during the normal use of an app. Rather than modifying the application or altering its behaviour, we focus on how it interacts with the device and external servers

This allows us to document what data is transmitted and to whom. Throughout this handbook, we refer to this approach as network forensics.

This type of approach is sometimes described as black-box testing: analysing a system from the outside, without access to its internal code. While it does not reveal how companies ultimately process the data on their servers, it can provide useful indications based on what is being transmitted.

2.3.1 Technical Set-Up

To carry out the analysis of a mobile app, a specific technical setup is required. The aim is to capture encrypted network traffic in a way that reflects real usage as closely as possible.

PREPARATION

We use dedicated Android devices configured for this purpose

The original version of the app (from the Google Play Store) is installed.

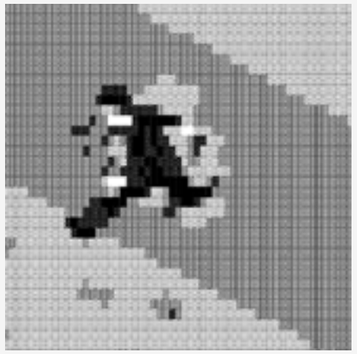
This setup allows us to observe data flows that would not be visible on worker devices.

INTERCEPTION INFRASTRUCTURE

The collection relies on a “machine-in-the-middle” (MITM) approach, which enables us to observe communication between the app and external servers:

- ↘ **Traffic routing:** network traffic is directed through a secure tunnel to a researcher-controlled machine
- ↘ **Proxy tool:** software such as mitmproxy captures requests and responses
- ↘ **Decryption:** a locally installed certificate allows encrypted (HTTPS) traffic to be inspected before being forwarded

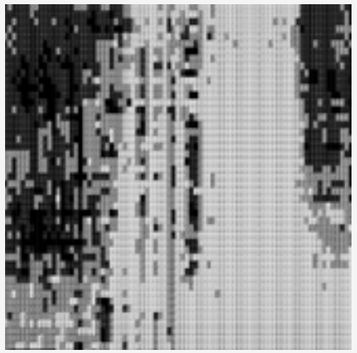
HANDLING SECURITY PROTECTIONS



Many apps include protections that prevent this type of observation. In such cases, additional steps may be needed to enable analysis without changing the app’s core functionality:

- ↘ **System-level access** to the device
- ↘ **Runtime tools** that adjust how the app verifies secure connections

DATA CAPTURE AND CONTEXT

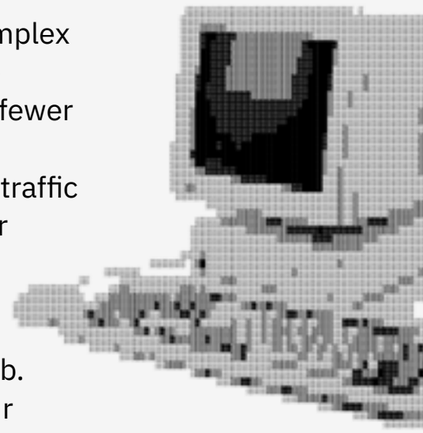


Once a worker logs in with their account, data collection begins:

- ↘ **Traffic logs:** records of network requests, including both metadata and transmitted content (e.g., location data or device identifiers)
- ↘ **Screen recording:** captures on-screen activity to help relate data flows to user actions

BROWSER ANALYSIS

While the previous section covered the more complex mobile case, analysis of web apps running in the browser is also possible. This scenario presents fewer challenges because the browser itself offers the tooling necessary to record, analyze, and export traffic data in HAR format. Several options also exist for screen recording



In practice. the setup involves only the browser, configured to collect the traffic data of a given tab. To learn more, refer to the documentation of your browser.

2.3.2 Types of Experiments

To document how platforms exercise control, we distinguish between two main modes of data collection based on the worker's activity status during the investigation. Both rely on the same core technical setup, network interception via a man-in-the-middle configuration, and screen recording, but capture different working contexts.

OFF-WORK EXPERIMENT:
MONITORING WORKERS AT REST

In an "off-work" experiment, the worker is not actively performing work-related tasks. The app may remain open or running in the background, but the worker is typicallyin an "offline" or inactive state.

- **Objective:** Observe what data is accessed and transmitted outside active working hours
- **Focus:** Background activity and passive data collection
- **Key findings:** This setup can reveal forms of continuous or low-visibility tracking. For example, in one case involving a food delivery app, GPS coordinates were transmitted at regular intervals even when the worker was not online or available for orders
- **Strategic value:** Helps assess whether data collection extends beyond what is strictly necessary for the execution of work, including potential sharing with external services
- **Practical note:** These experiments are often easier to schedule, since workers remain in an offline mode and do not have to be on shift or ready to work. They are also less likely to trigger security mechanisms that are activated during real-time task execution.

AT-WORK EXPERIMENT:
MONITORING REAL-TIME WORK

In "at work", or live experiment, the worker is actively engaged with the platform, for example, receiving tasks, moving through space, and completing work.

- **Objective:** Observe app behaviour during real working conditions, including task allocation and location-based interactions
- **Focus:** Real-time tracking, task management, and potential signals of automated decision-making
- **Complexity:** These experiments tend to be more sensitive and technically demanding, as they need to be carefully scheduled around the worker's availability; typically when they are willing to work or have a shift planned.
- **Technical challenges:** Some applications include additional device-level checks that can detect or restrict modified inspection environments during active use

Taken together, off-work and at-work experiments provide complementary perspectives. If you don't know the app at all, it can be a good idea to is often preferable to begin with the off-work setup, as it is easier to establish baseline data flows. The at-work experiment can then follow to address additional research questions. Combined, they offer a more complete view of how platform systems may extend forms of control both within and beyond formal working time.

PLANNING FOR DIFFERENT OPERATIONAL MODELS

When designing these experiments, it is important to understand how a given system defines “working time.” This shapes how data collection is framed and justified. Both mobile apps and computer-based software typically follow one of three operational models:

OPERATIONAL MODELS

- **Shift-based systems:** The worker operates within fixed or negotiated time slots. Data collection outside scheduled shifts is often harder to justify as necessary for service delivery.
- **Online/Offline systems:** The worker manually signals availability. Our investigations have often shown that even when marked “Offline,” mobile apps or software may continue collecting data such as location or device activity.
- **Always-on systems:** Common in platforms with continuously available tasks. The boundary between “working” and “not working” becomes blurred, and background data collection may extend across most of the time the software is active.

DOCUMENT THE USER EXPERIENCE!

Remember to save contracts, mail, schedules and to take screenshots of the shifts. These boundaries might be very clear to you, but not too the person that might handle your evidence to.

2.3.3 Storing Collected Data

While participation in an investigation typically involves limited risk for workers, caution is still necessary. Building trust depends on ensuring that all collected data is handled in a transparent, secure, and professional way.

Key practices include:

- **Store data on controlled infrastructure:** All data should be kept on systems controlled by the research team (e.g., dedicated servers or local machines). Third-party cloud services are avoided during collection to reduce unnecessary exposure.
- **Store consent forms:** Each participant signs a consent form outlining the purpose of the collection. A copy is stored alongside the technical data for accountability.
- **Define retention rules in advance:** Partners agree in advance on storage duration and sharing conditions. Once analysis and follow-up actions are complete, raw data is deleted according to the agreed retention policy.

2.3.4 Legality and Risks

Workers are often concerned about the legal implications of analysing workplace apps. This is understandable: intercepting and inspecting network traffic is not something most people do every day.

The key point is that the main legal questions are usually not about observing network traffic itself, but about how the information obtained through that analysis is later used.

IS NETWORK TRAFFIC ANALYSIS LEGAL?

We are not aware of any general prohibition on a user analysing network communications generated by software running on their own device and account in order to understand how the system operates. As with most legal questions, the answer depends on the country and the specific circumstances. However, there are several reasons why we consider this approach legitimate.

- **The worker remains in control.** Workers should never share their passwords or account credentials with researchers, unions, lawyers, or other representatives. Others may prepare technical tools and help interpret the results, but the worker remains in control of the account at all times.
- **The analysis is passive.** The methodology does not modify software, bypass security measures, interfere with the service, or gain access to information that the worker is not entitled to see. It simply observes information exchanged between an app and a device controlled by the worker.
- **The goal is to understand the system.** Workplace apps increasingly allocate work, monitor performance, and make decisions that affect workers' income and working conditions. Traffic analysis is a way of understanding how these systems operate when meaningful transparency is unavailable.
- **What matters most is how the information is used.** Any disclosure should be carefully considered and serve a legitimate purpose. Sharing findings with lawyers, unions, regulators, courts, or other public authorities is different from unrestricted public disclosure.

This handbook does not claim that every use of network traffic analysis is lawful in every situation. However, we believe that workers have a legitimate interest in understanding how systems that affect their working lives operate.

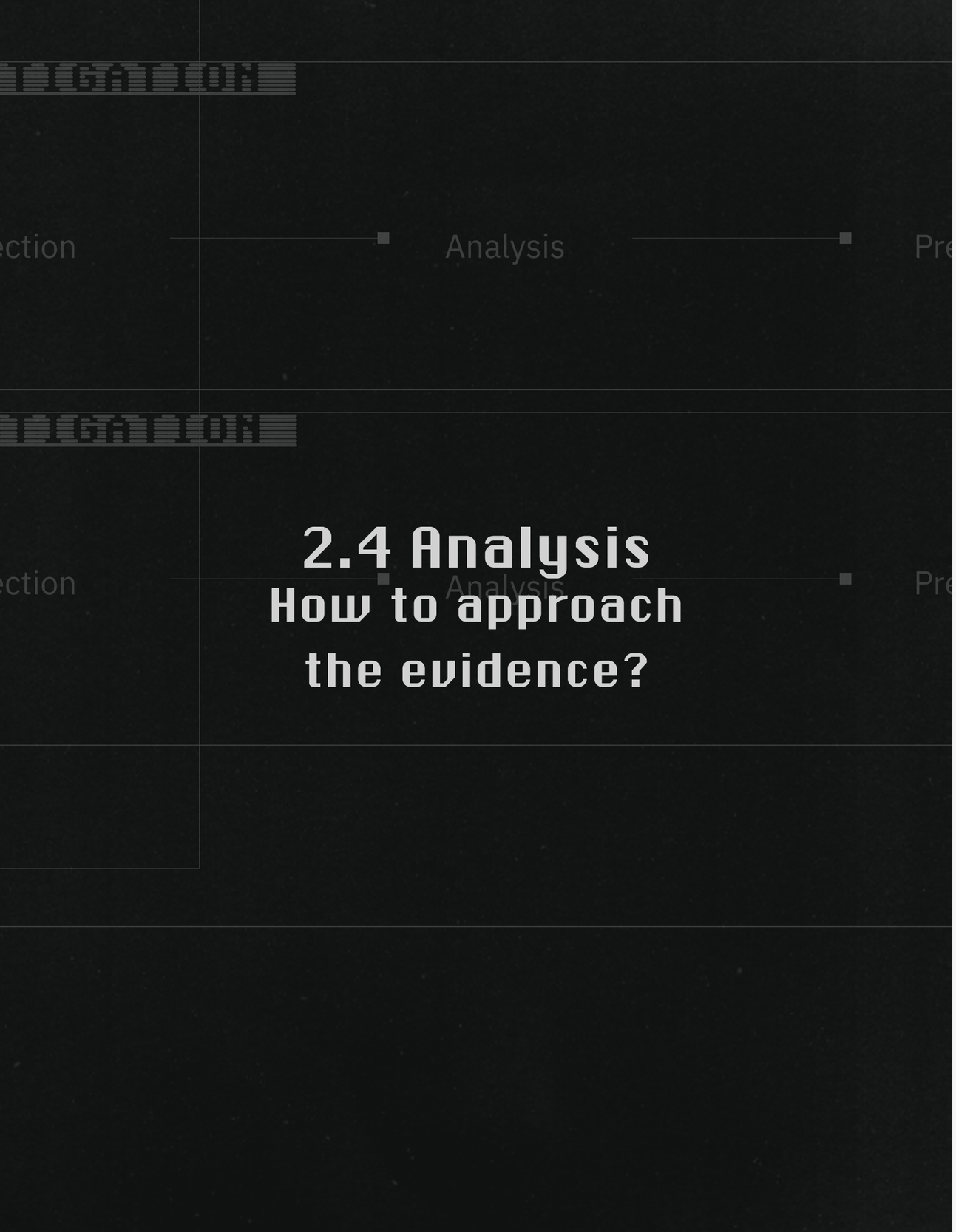
WHAT ARE THE RISKS TO THE WORKER?

The main risk is not the technical analysis itself, but the possibility that an employer becomes aware that it is taking place. The methodology is not designed to announce its presence to the platform. The application continues to communicate with the company's servers in the normal way, while the analysis is carried out locally on the worker's device. In many cases, this makes the activity difficult to detect.

At the same time, no technical method should be assumed to be completely invisible. Detection appears unlikely in many situations, but it cannot be ruled out entirely. Employers may also learn about the analysis through other channels, such as workplace discussions, organising activities, or later legal proceedings.

If an employer becomes aware of the analysis, they may argue that it violates company policies, terms of service, or contractual obligations. Whether such claims are justified will depend on the circumstances. However, employers do not always need to be legally correct in order to create difficulties for workers.

Possible consequences include workplace pressure, disciplinary action, dismissal, or legal threats. These risks are not unique to traffic analysis and may arise whenever workers challenge opaque management practices or seek greater accountability. Workers should therefore consider their individual circumstances before participating. Where possible, it is helpful to discuss participation with trusted colleagues, unions, worker representatives, or legal advisers.



2.4 Analysis
How to approach the evidence?

→
After the collection phase, we are left with a combination of network traffic data, worker feedback, and contextual notes from in-person workshops or remote sessions. The next step is to make sense of this material. In practice, we use two complementary ways of approaching the analysis:

(1) Data-first approach: starting from the dataset itself and exploring it to identify patterns, anomalies, or unexpected behaviours.
(2)Hypothesis-first approach: starting from a specific question or assumption about how the system might behave, and then looking for evidence that supports or challenges it.

Most analyses move between these two approaches rather than following only one.

2.4.1. Data-First Approach

In a data-first analysis, we begin with the traffic dataset and explore it without a predefined hypothesis. The aim is to identify elements that appear unusual or informative, and use them as entry points into understanding system behaviour.

Typical points of attention include:

- **Sensitive or unexpected data:** identifying values such as identifiers, location data, prices, or other information that may be broadly shared or transmitted
- **External connections:** reviewing which third-party services are contacted, including less familiar endpoints that may indicate additional data flows
- **Payload size and structure:** observing larger or unusual requests that may contain richer datasets or bundled activity logs
- **Emerging patterns:** noting recurring behaviours or anomalies that can be followed up on in later stages of analysis

This approach can help surface issues that were not anticipated in advance and supports a more exploratory understanding of how the system behaves in practice.

At the same time, it can be time-consuming and requires the ability to interpret both technical network data and its potential legal or organisational relevance.

To practice this kind of investigation, you can look at the traffic of simpler apps you know well and use every day. Compare your actions on the interface with the traffic logs in real time, and how specific features translate into specific details in the logs.

2.4.2 Hypothesis-First Approach

A hypothesis-first analysis begins with a provisional assumption about how a system might behave, based on earlier findings, worker accounts, or broader expectations about platform operations. We then explore the dataset to identify evidence that may support or challenge this assumption.

In practice, hypotheses often emerge from a combination of sources, including workers' experiences, prior experiments, and recurring patterns observed across investigations. This approach helps bring structure to the analysis and ensures attention is focused on specific, testable questions.

One advantage of this approach is that it is relatively easy to systematise and, in some cases, automate. It also provides a direct link to workers' experiences, allowing their concerns to guide the direction of analysis ina more structured way.

Its main limitation is that it tends to focus attention on what is already anticipated. As a result, it may overlook less visible or unexpected forms of data practice that fall outside the initial assumptions.

The following examples illustrate how a hypothesis can be translated into a concrete line of analysis.

THE APP COLLECTS WORKERS' LOCATION OUTSIDE WORKING TIME

A common concern is whether location data is collected beyond active working periods. Given its sensitivity, such data can reveal detailed aspects of private life, and its collection may raise questions of proportionality and necessity. Within network traffic, location data may appear in different forms, including:

- Fields such as lat, long, latitude, longitude, location, or similar
- GPS coordinate pairs (e.g. 51.44492, -0.12022)
- Encoded formats such as geohashes or compressed location strings

Once identified, it is useful to consider the broader context:

- ↘ Whether the data appears once or continuously
- ↘ At what moments is it transmitted (e.g., active shifts, inactivity, background use
- ↘ What seems to trigger the transmission

This helps assess whether location tracking is limited to operational needs or extends into more continuous forms of monitoring.

THE APP SHARES DATA WITH UNDISCLOSED THIRD PARTIES

Workplace apps often rely on external services, which are not always clearly identified in privacy policies. This line of analysis focuses on identifying which external entities actually receive data in practice.

A typical starting point is:

- ↘ Identifying all external request destinations in the traffic data
- ↘ Excluding services clearly operated by the platform itself
- ↘ Filtering out requests that do not involve data transmission (e.g., static content downloads)
- ↘ Comparing the remaining services with those disclosed in the documentation

Where services appear that are not mentioned in privacy materials, this may indicate gaps in transparency. Further inspection of the data exchanged can help clarify their role.

THE APP SHARES SENSITIVE WORKER DATA BEYOND WHAT IS NECESSARY

This analysis looks not only at which third parties receive data, but also at what kind of data is shared. Even when services are disclosed, they should ideally only receive information necessary for their stated function.

Many third-party tools serve technical purposes such as analytics, performance monitoring, or error reporting. However, they may still receive data that goes beyond what is strictly required.

A useful way to approach this is to examine each service in turn:

- ↘ What is the intended function of the service, based on documentation or external information?
- ↘ What data is actually being transmitted to and from it?
- ↘ Does any of this data appear excessive or unrelated to that function?

This process often involves reviewing request and response payloads for elements such as identifiers, contact details, location data, or operational information (e.g., shifts, orders, or payments). Over time, this can help build a shortlist of cases that may warrant closer examination.

LIMITATIONS OF OUR INVESTIGATIVE APPROACH

When selecting an investigative strategy, it is important to understand what our approach can and cannot deliver. The method is designed to produce meaningful, high-impact evidence with relatively limited resources, but it operates within clear technical and legal constraints.

- **Black-box limitation:** Because analysis is external, it is not possible to determine exactly how data is processed once it reaches company servers.
- **Limited insight into algorithms:** While we can detect signals of automated decision-making (e.g., scoring or demand indicators), we cannot reconstruct the underlying logic or model behaviour.
- **Difficulty proving discrimination:** Identifying patterns is possible, but demonstrating discriminatory outcomes usually requires larger samples and longer-term, repeated observations.
- **Security interference:** Some apps use protections (e.g., device integrity checks) that can block or restrict analysis tools, limiting what can be observed, sometimes to background activity only.
- **App volatility:** Frequent updates or changes in encryption can temporarily disrupt the setup or affect comparability over time.
- **Account dependency:** Observations are limited by what a specific worker account can access, meaning some data flows may not be visible if certain functions or tasks are not available.

3. HOW TO TRANSLATE EVIDENCE INTO OUTCOMES?

3.1 Presentation
How to share the findings?

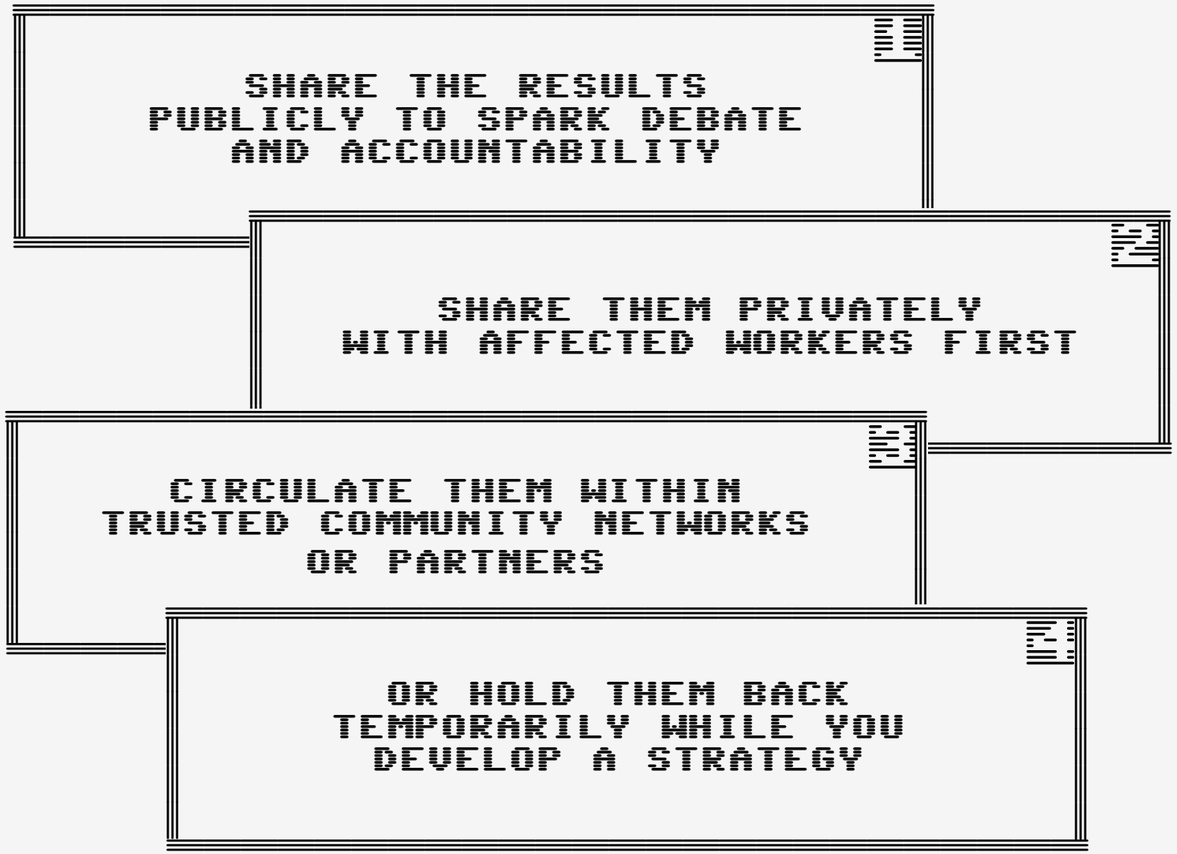
Presentation

Presentation → Action

→
After completing an investigation, you will receive a short report summarising the technical evidence. What happens next is not automatic: it depends on your goals, your context, and the alliances you want to build. This is a good moment to pause and reflect, not just on what the data shows, but on what it makes possible.

Think back to your original assumptions about the app. Did the findings confirm them, or challenge them? Was the scale of data collection larger than expected? Were you surprised by how many third parties are receiving data directly from your phone?

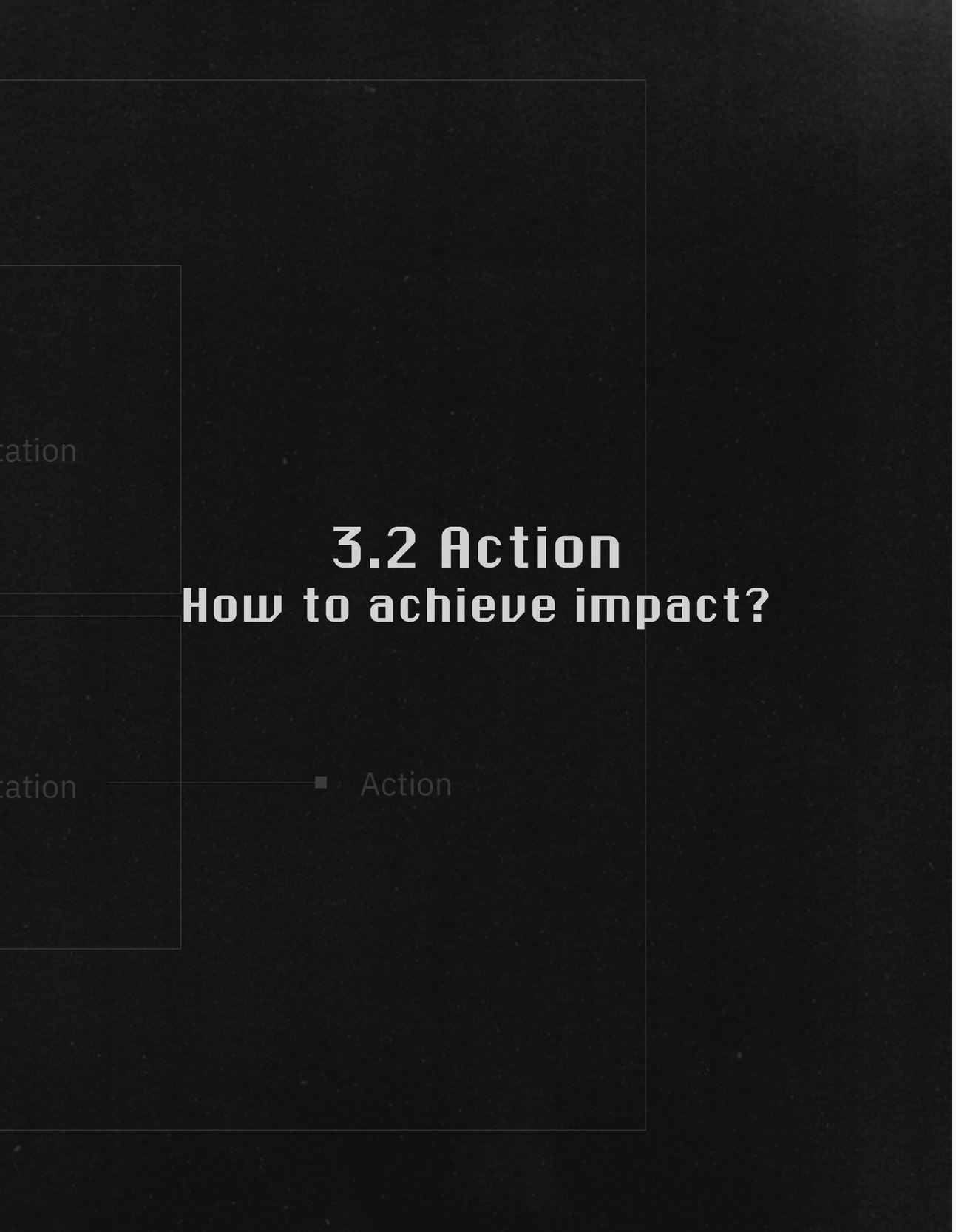
From here, the key question becomes: who needs to know?
There is no single correct answer. You might decide to:



Each choice carries different risks and opportunities. But in most cases, the evidence is not an endpoint: it is a starting point for collaboration. It can become the basis for joint research, coordinated advocacy, legal strategies, or cross-border alliances between workers and their representatives.

Importantly, sharing does not have to mean going public immediately. Sometimes the most strategic move is to first build relationships, test interpretations together, and decide collectively how and when to act.

In most cases, the evidence
is not an endpoint:
it is a starting point for collaboration.



→
Reversing.Works is one way of documenting live data flows, but it sits within a much broader ecosystem of investigative and auditing practices. Different situations call for different methods, and often the strongest insights come from combining them.

3.2.1 Action: Further research and collaborative investigation

Reversing.Works is one way of documenting live data flows, but it sits within a much broader ecosystem of investigative and auditing practices. Different situations call for different methods, and often the strongest insights come from combining them.

This is why collaboration matters. Groups such as Worker Info Exchange, PersonalData.io, and the Workers' Algorithm Observatory have been developing and refining independent audit methods that complement technical interception work with legal, ethnographic, and data-driven approaches. Together, these methods help build a more complete picture of algorithmic management.

COMPLEMENTARY INVESTIGATIVE METHODS

- **Data Subject Access Requests (DSARs):**
  Under the GDPR, workers have the legal right to demand a copy of their personal data from a company. This can reveal stored profile information, order histories, and internal metrics. A significant drawback is that companies often provide incomplete or illegible data or fail to respond within the legal timeframe. For example, Worker Info Exchange has used DSARs as a core tool to gather the evidence necessary to challenge platform companies in court, such as in cases involving Uber and Ola in the Netherlands, where the data helped contest opaque management decisions.

- **Data Scraping:**
  his involves workers taking regular screenshots of their application or using automated software to record what the app displays over time. This is particularly useful for documenting dynamic changes, such as shifting pay rates or surge pricing, though it typically requires participation from a large number of workers to be statistically significant. For example, the Workers' Algorithm Observatory (WAO) utilizes these methods to aggregate data from many participants, turning individual screenshots into a dataset that can reveal systemic patterns in how algorithms manage workers.

- **Cross-source data triangulation:**
  A method that compares multiple datasets measuring the same phenomenon to assess consistency and bias. For example, a 2024 study by PersonalData.io used documentary analysis to compare Uber's declared mileage records against external routing algorithms to uncover discrepancies in driver compensation. In this investigation in Geneva, researchers compared state-validated mileage, platform-reported data, and open-source recalculated mileage to prove that platform data is often not neutral and can put workers at a disadvantage.

Evidence rarely speaks for itself:
it becomes powerful when it is shared,
discussed, and used collectively.

3.2.2 Action: Raise Awareness and Build Collective Pressure

Evidence rarely speaks for itself: it becomes powerful when it is shared, discussed, and used collectively.

At this stage, it is worth considering whether and how to make findings more widely visible. Depending on your strategy, this might include:

- **Starting conversations** with colleagues who may be experiencing the same systems
- **Connecting** with workers using the same platform in other companies or countries
- **Sharing findings** with journalists or media organisations
- **Launching public awareness campaigns** or coordinated advocacy efforts
- **Engaging in collective actions** such as petitions, protests, or “name and shame” initiatives

In some cases, the first step may be internal: bringing concerns to employers or managers, ideally supported by trade unions or worker representatives. Evidence about data practices can strengthen these conversations and help formulate concrete demands such as limits on surveillance, clearer transparency, or safeguards around algorithmic decision-making.

But when dialogue is not enough, evidence can also become a tool for pressure and mobilisation. What often begins as individual surprise can turn into collective recognition: if one person is affected, others usually are too.

3.2.3 Action: Legal Pathways

Start by considering whether your evidence points to possible data protection violations. It is often not easy to assess on your own whether the General Data Protection Regulation (GDPR) has been breached, but you are not expected to do this alone.

You may find useful guidance by looking at existing cases and documentation in the food delivery sector, where similar patterns have already been analysed. If you want support at this stage, reach out to others working on similar issues. Trade unions can offer legal expertise, worker representation, and experience with collective claims. You can also connect with digital rights organisations such as noyb, Worker Info Exchange, PersonalData.io, and the European Digital Rights (EDRi) network. These groups combine legal, technical, and advocacy skills to help workers challenge algorithmic systems and build stronger accountability cases together.

Your evidence may indicate that the company you work for has violated data protection laws or labour regulations. Legal action can take different forms, but one of the most accessible first steps is to submit a complaint to your local Data Protection Authority (DPA).

Importantly, you can submit a complaint even if you are only suspecting a violation. You do not need to prove your case or provide legal arguments. The process is free, and you only need to describe what you have observed and share the evidence you have collected. DPAs are required to review complaints and, in many cases, to investigate further.

PATH 1: SUBMIT A COMPLAINT TO DATA PROTECTION AUTHORITIES (DPAS)

Filing a complaint with your national DPA is often the most straightforward legal step if you suspect data protection violations. **The process is usually free and does not require a lawyer.**

If a company processes your personal data, you are considered a data subject. **This gives you the right to submit a complaint either in your country of residence or in the country where the company's main EU headquarters is located**. This applies regardless of whether you are formally employed, self-employed, or working without a contract.

Procedures vary between countries, but **many DPAs allow online submission.** When filing a complaint, focus on clearly describing the practice that concerns you and include concrete evidence such as screenshots, screen recordings, or traffic data collected during your investigation. **You do not need to cite legal provisions or build a formal legal argument.**

In some EU countries, trade unions, works councils, or worker representatives can submit complaints on behalf of workers. Even if you are not part of these structures, you can still contact the DPA directly by email or online form. Some authorities may also open investigations on their own initiative, although they are generally not required to provide updates unless a formal complaint is submitted.

DPAs can impose sanctions such as fines, order companies to stop unlawful practices, and require compliance measures.

Data Protection Violations in Food Delivery:
A Practical Guide

Use this checklist to identify common data protection violations in food delivery platforms. Look for patterns, document evidence, and compare experiences across workers.

1. LOCATION TRACKING OUTSIDE WORKING HOURS

WHAT TO LOOK FOR?

- ☐ Rider apps that continue tracking GPS location when you are not working
- ☐ Tracking that remains active in the background during evenings, weekends, breaks, or days off
- ☐ No clear option to fully disable location tracking outside shifts

WHY IT MAY BE A VIOLATION?

- ↘ **Data minimisation** (Art. 5(1)(c) GDPR): Companies should only collect data necessary for the job. Continuous tracking goes beyond what is needed for delivery work.
- ↘ **Purpose limitation** (Art. 5(1)(b)): Tracking outside working time usually has no legitimate work-related purpose and therefore lacks justification.

2. SHARING DATA WITH THIRD PARTIES

WHAT TO LOOK FOR?

- ☐ Your location, schedule, ratings, or performance data being shared with insurers, analytics firms, subcontractors, or other partners.
- ☐ No clear explanation in the app or contract about who receives your data
- ☐ Discovering third-party access only indirectly (e.g., through investigation or experience)

WHY IT MAY BE A VIOLATION?

- ↘ **Lawful basis requirement** (Arts. 5(1)(a), 6): Personal data can only be shared if there is a valid legal basis.
- ↘ **Transparency rules** (Arts. 13–14): Workers must be clearly informed about who receives their data and for what purpose.
- ↘ **Processor rules** (Art. 28): If third parties process worker data, there must be a formal contract defining responsibilities and limits.

3. AUTOMATED DECISION-MAKING (ALGORITHMIC MANAGEMENT)

WHAT TO LOOK FOR?

- ☐ Orders being assigned automatically without explanation or human involvement
- ☐ Algorithmic scoring systems that affect access to shifts, bonuses, or pay
- ☐ Sudden account suspensions or penalties triggered by automated systems
- ☐ Little or no ability to challenge or review decisions

WHY IT MAY BE A VIOLATION?

- ↘ **Automated decision safeguards** (Art. 22 GDPR): Workers should not be subject to decisions that significantly affect their work without human oversight or safeguards.
- ↘ **Transparency requirements** (Arts. 13–15): Workers must be informed about how automated systems work and what impacts they have.
- ↘ **Fairness principle** (Art. 5(1)(a)): Hidden ranking or scoring systems can create unequal or discriminatory outcomes, especially when not open to review.

However, these procedures usually do not provide individual compensation to workers.

PATH 2: SUE THE COMPANY FOR BREAKING DATA PROTECTION OR LABOUR LAWS

If you believe your data protection rights were violated, you can also bring a case to court and seek compensation. This route exists alongside complaints to DPAs and is often stronger when combined with collective organising or union support.

Court proceedings usually require legal assistance and may involve costs. The relevant court depends on the national legal system and the type of claim. Evidence collected during your investigation, such as screenshots, recordings, or traffic data, can be crucial in showing how a company collects, processes, or shares data.

Across EU Member States, two main legal pathways are typically relevant:

- **Labour courts** deal with disputes linked to employment relationships. In some countries, workers can challenge unlawful monitoring or excessive data collection at work through this route. Evidence about data practices may also support broader claims, such as unfair working conditions, discrimination, or unpaid wages. Trade unions or works councils may also bring cases, especially where workers were not properly informed or consulted about data processing.

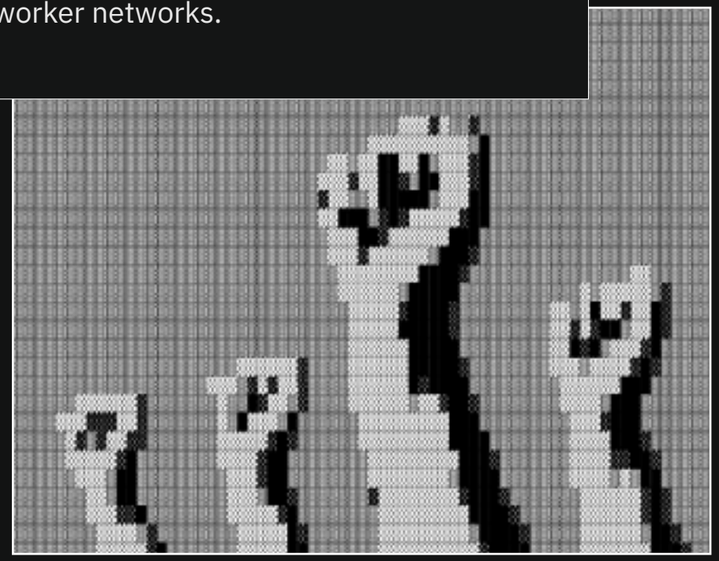
- **Civil courts** handle compensation claims where unlawful data processing has caused harm, including financial loss, reputational damage, or distress. Under EU law, individuals can seek compensation for both material and non-material damage resulting from violations of their rights.

Procedures, available courts, and possibilities for collective action vary across EU Member States. If you are considering this

STRATEGIC LITIGATION

Filing a complaint with a DPA or pursuing a court case can have broader effects beyond your individual situation. Strategic litigation can:

- Encourage companies to change practices and comply with the law more carefully.
- Clarify how data protection and labour laws apply in emerging contexts, such as digital monitoring or algorithmic management.
- Support wider advocacy efforts by engaging civil society organisations, NGOs specialising in labour rights or data protection, and worker networks.



STRATEGIC LITIGATION CAN THUS STRENGTHEN BOTH INDIVIDUAL AND COLLECTIVE RIGHTS IN THE WORKPLACE.

MOVING
FORWARD

Moving forward

This handbook has set out the core elements of a digital workplace investigation: how to plan and conduct data collection, how to analyse technical evidence, and how to translate findings into action. The approach is grounded in practice and refined through years of collaboration with workers, unions, NGOs, and technical experts across Europe.

The methodology described here is a starting point, not an endpoint. No single actor has all the expertise needed to challenge algorithmic management effectively. Workers bring direct experience of the systems under scrutiny. Technical experts contribute the tools and methods to make those systems legible. Unions and NGOs provide the organisational capacity and legal knowledge to act on what is found.

For those considering next steps, the path forward depends on your role and context. Workers and collectives with concerns about workplace apps should document their experience and connect with a partner organisation. Unions and labour NGOs should consider integrating digital investigations into existing practice, starting with a supported collaboration. Technical experts are encouraged to reproduce and extend the methods described here, and to connect with labour organisations working on concrete cases.

We welcome contact from anyone working in this space. Whether you are looking to start an investigation, share expertise, or build connections with others doing similar work, we are glad to help facilitate.

Reach out to us at Reversing.Works.

GLOSSARY

ALGORITHMIC MANAGEMENT

Following Eurofound, algorithmic management is defined as "the use of computer-programmed procedures to monitor, organise, direct and evaluate workers, relying on the collection and processing of worker data to enable automated or semi-automated decision-making."

Other definitions in the literature place greater emphasis on different aspects: the opacity of these systems and the resulting power imbalances they create for workers (Mateescu & Nguyen, Data & Society, 2019), their role in enabling new forms of remote workforce control at scale (Möhlmann et al., 2021), and the ways in which they blur the boundary between management and surveillance.

AUTOMATED DECISION-MAKING (ADM)

Under GDPR Article 22, automated decision-making (ADM) is defined as "a decision based solely on automated processing, including profiling, which produces legal effects." Workers have the right not to be subject to ADM and to have decisions with significant effects reviewed by a human. In the workplace, ADM includes practices such as algorithmic task allocation, performance scoring, and account suspension.

DATA PROTECTION AUTHORITY (DPA)

Independent public authorities responsible for enforcing data protection law, including the GDPR. Each EU Member State has its own DPA. They investigate complaints, issue fines, and can order companies to change their practices. Workers can submit a complaint to their national DPA free of charge and without legal representation, making them one of the most accessible routes to challenging unlawful data practices in the workplace

DATA SUBJECT

Any identified or identifiable natural person whose personal data is being processed. Under the GDPR, any individual whose data is collected, stored, or used — including workers — is a data subject, regardless of their employment status or contractual relationship with the organisation processing their data. Being a data subject carries enforceable rights, including the right to submit a Data Subject Access Request (DSAR) to obtain a copy of one's personal data and information on how it is processed.

MACHINE-IN-THE-MIDDLE (MITM)

A technique that intercepts communication between two parties — in this context, between a workplace app and external servers — allowing the data exchanged to be observed and recorded. The interception is invisible to the app and does not alter its behaviour. Tools such as mitmproxy implement this technique to capture network traffic for analysis.

NETWORK FORENSICS

The systematic capture and analysis of network traffic to produce reproducible, evidential findings. Originally developed in cybersecurity and criminal investigation, network forensics is applied here to document how workplace apps collect and process workers' personal data and assess compliance with data protection law, without modifying the application or accessing its internal code.

PLATFORM WORK

Following Eurofound, platform work is defined as "the matching of demand and supply of paid work through an online platform using an algorithm." The EU Platform Work Directive (2024/2831) similarly defines it as work organised or facilitated by a digital labour platform, regardless of the contractual relationship or employment status of the worker. Across both definitions, algorithmic management is the central and defining feature.

We are Reversing.Works, a transdisciplinary research team working to expose and challenge algorithmic management in the digital workplace.

staff@reversing.works

reversing.works