International
Labour
Organization

ILO Brief

Improving Workers' Data Rights

Introduction

This brief discusses how data extraction from our private life and work life can influence our work opportunities, the balance of power between management and labour, as well as the rights workers should have to these data to prevent a narrowing of labour market opportunities.

Everything digital extracts and/or produces data. From your use of social media, your credit card payment information, your shopping habits, what websites and apps you use and when, and on to the 14 sensors on your smartphone that extract data about your location, the sound and temperature around you, your speed of travel and much more. All of this data is used to infer things about us – as citizens but also as workers. To profile us and make predictions about us for advertisement, but also for the manipulation of thought, the availability of jobs to an individual and ultimately to how inclusive and diverse the labour market is.

Importantly, it is not just your life and career that is affected by this data extraction. As data gets accumulated, it is used to compare people or groups of people against endless other criteria. For example, customer ratings in relation to worker characteristics, types of friends with likelihood of unionisation. Body mass index with worker speed. Accent, postcode and perceived trustworthiness. The algorithmic systems used to find all of these correlations, probabilities, predictions and differences are constantly getting more elaborate as the amount of data exponentially grows. What you do, in other words, without you ever knowing, affects the lives of others.

Data at work

Exacerbated by the COVID19 pandemic, the trend towards data-driven workplaces has only grown. All digital services and systems in workplaces extract data on workers. We can identify 5 ways that this takes place:

Data at work

Direct collection
from job candidates, employees, customers

Sensor derived data
via handheld devices, wearables, or equipment

Purchased data profiles/sets
from third parties

Audio and visual data
from CCTV, phone calls, facial recognition

Data traces extraction
from computer and network systems

- **Direct collection:** Your CV contains lots of valuable information. From your previous employers, to your education, maybe even spare time interests and other activities. Employers can also directly collect data from their customers (what they buy, how often, what goods or services they look at on the website etc.) or from their current employees (for example how often they are sick, how many hours or shifts they work etc.).
- **Purchased data profiles**: There are many so-called data brokers out there in the world whose whole business model is concerned with the buying, bundling and selling of data sets. These can be aggregated traffic data sets, or data about the "trustworthiness" of particular groups of people, or profiles about credit scores, health or education levels per geography or socio-economic status.
- **Data traces extraction:** When you log on to your work email or server you are leaving a trace of your activities. What time did you log on, which documents have you accessed? Also, some systems, such as Office365, create reports of how "productive" you have been, how much "concentration" time you have had etc. Does the management see these measures too?
- **Sensor derived data:** Some offices have sensors throughout the building: Under desks to message how often that desk is used and vacated. On doors to see how often a room is used, or not. Some workers have to use handheld scanners or wearables such as a Fitbit or location tracking systems. All of these produce data that is, or can be, used by management.
- **Audio and Visual Data:** Other types of data are derived from audio-visual systems. Call center workers' tone of voice and what they say are measured and evaluated. Mobile phone call tapping. CCTV or Facial recognition is used to locate and identify workers. Although highly criticised, some of these systems have been used to predict the emotional state of mind of workers: are they tired, do they look sad, frustrated, happy or nervous?

Regardless of the means of extraction, digital monitoring and surveillance systems gather data about workers and their actions and non-actions. Whilst monitoring is not new, the digital nature of the current systems have particular characteristics that will have an influence on how unions should relate to them. Imagine a system that monitors factory floor workers' productivity through surveillance cameras and handheld sensors. *Firstly*, the system is impossible to avoid as it is embedded into work processes and devices. *Secondly*, the monitoring is comprehensive - it collects a large amount of data from multiple sources. *Thirdly*, management gets instantaneous information as the data is collected in real time. *Fourthly*, the system is interactive, offering real time communication and feedback – in our case here through factory floor screens showing how the productivity of each and every worker.

Employers can use these data to measure workers' productivity and efficiency (however that is defined). They can make elaborate calculations on the likelihood that you, for example, will meet your targets, be appreciated by customers, be fast-paced, or are dedicated to the job. Or they can use this to make predictions about you: are you likely to leave the company soon, fall ill, become slower, or join a union.

What exactly the employers use the data for depends on the *purpose* of the systems they deploy and the data analyses they conduct. In some cases, workers might agree to the extraction of data. For example, workers might support the extraction of data for health and safety purposes to avoid accidents or to measure working time to avoid stress and burnout. What is important is that the workers know about and have influence over whether data extraction should take place, what the purposes of any data extraction are, how the data is used, and what happens to the data afterwards. Brief 2 discusses the already lived harms and impacts of data and algorithms on workers.

The Political Economy of Data Extraction

Although workers and employers in principle could agree on the purposes of data extraction and analysis, a wider issue is at stake. Namely, do we really want our actions to be quantified, turning our labour into numerous data points that might or might not be abused? If workers are perceived more as numbers or points against a statistical norm rather than humans, how will this affect human rights and workers' rights?

A common narrative is that data is "the new oil" - an extracted resource that is valuable, but if unrefined cannot really be used. Hence, data must be analysed and bundled. It needs to become an asset that can be repurposed to add value in production and service chains. This narrative thus asserts that data is a commodity that can be bought and sold. Following that assertion, workers' data can be monetised. However, viewing workers' contribution to this means of production in such monetary terms, and as some do, demanding on this basis a redistribution of the value-added back to the workers, only solidifies and maybe even justifies the commodification of labour.

Critiques of this economic perspective on data claim that data must be seen in a power and rights perspective. Those who collect the data, are those who win power over markets, competitors, citizens and workers. It is unilaterally their analyses, their stories that dominate and in turn manipulate what services, points of view, products are revealed to us individually irrespective of human rights and other moral considerations.

The acclaimed author of The Age of Surveillance Capitalism, Shoshana Zuboff, is adamant we should make what she calls "behavioral futures markets" illegal[1]. Here she refers to the trading of data inferences that are used to constantly manipulate our unsuspecting selves. As she describes, for data collectors to offer certainty to their clients they need huge amounts of data, and they need a variety of data to ensure their predictions and models are as accurate as possible. This leads to economies of scale and scope - and hence the concentration of power into the hands of a few, very wealthy global companies: Google, Meta, Apple, Amazon, Microsoft, Alibaba and Tencent.

Whilst data extraction in the economic perspective is only restricted by law (for ex data protection regulations), a rights-based approach stipulates that data can only be extracted if it respects the broader human rights suite. The OHCHR issued in 2018[2] a guidance note on the principles of a human-rights based approach to data. Here they recommended 6 key principles each with a number of sub-principles:

1. **Participation:** *Participation of relevant population groups in data collection exercises, including planning, data collection, dissemination and analysis of data*

2. **Data disaggregation:** *Disaggregation of data allows data users to compare population groups, and to understand the situations of specific groups. Disaggregation requires that data on relevant characteristics are collected*

3. **Self-identification:** *For the purposes of data collection, populations of interest should be self-defining. Individuals should have the option to disclose, or withhold, information about their personal characteristics*

4. **Transparency:** *Data collectors should provide clear, openly accessible information about their operations, including research design and data collection methodology. Data collected by State agencies should be openly accessible to the public*

5. **Privacy:** *Data disclosed to data collectors should be protected and kept private, and confidentiality of individuals' responses and personal information should be maintained*

6. **Accountability:** *Data collectors are accountable for upholding human rights in their operations, and data should be used to hold States and other actors to account on human rights issues*

For workers' these principles would entail that they have the right to be involved in what data is extracted, for what purposes it is used, that the data is representative and therefore not discriminative and that human rights are respected at all times. Are these rights afforded to workers in data protection regulations across the world?

Data Protection Regulation and Workers

Data protection regulations across the world are concerned with the processing of a subject's personal data, or additional in some, personally identifiable information[3]. According to UNCTAD, 19% of all countries in the world do not have data protection regulations in place[4]. In relation to workers' data specifically, data protection regulations across the remaining parts of the world can be divided into three broad categories. Those that include specific articles on workers' data (such as the European General Data Protection Regulation - the GDPR), those that implicitly do such as most countries in Africa, Latin America and Asia Pacific, and those that explicitly exclude workers (such as the California Consumer Privacy Act of 2018 - the CCPA and partially the Australian Privacy Act of 1988[5]).

Most data protection regulations belong to the second category[6]. Here all legal requirements related to data privacy apply to the collection, processing, transfer and use of employee data. In addition, the vast majority rely on workers' 'informed consent[7]' for the extraction and use of worker data by employers. This is contrary to the

[1] https://www.project-syndicate.org/onpoint/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01?barrier=accesspaylog
[2] https://www.ohchr.org/documents/issues/hrindicators/guidancenoteonapproachtodata.pdf
[3] https://techgdpr.com/blog/difference-between-pii-and-personal-data/
[4] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[5] https://www.lexology.com/library/detail.aspx?g=0f6d20a7-a6b1-4980-aa0e-a98f1d637d38
[6] See this eBook for a good overview: https://www.mayerbrown.com/ebooks/A-Global-Guide-to-Employee-Data-Privacy/#/spreads/1
[7] The GDPR states that consent must be 'freely given, specific, informed and unambiguous. This means that the data subject must be aware that they are consenting to have their data processed and should not be forced into giving consent. Recital 32 - Conditions for Consent - General Data Protection Regulation

minor exceptions,[8] informed consent is therefore not a legal basis for processing workers data in the GDPR.

The third category which explicitly excludes workers is not common although several data protection bills currently under negotiation in the US are seeking to exclude workers in the same manner. The CPPA was amended by Assembly Bill 25 (AB-25) in 2019, which removed employers' obligations towards California residents in their position as job applicants, employees, persons who are autonomous contractors, corporate officials and executives[9]. Regardless of AB-25 exemptions, employers are still obligated to notify consumers *including members of their workforce* as well as job seekers about the categories of personal information they collect and the purposes of its utilization at or before the point of collection.

In summary, with the exception to a certain degree of workers covered by the GDPR, workers' data rights are poorly defined in data protection regulations across the world. Whilst the majority of data protection regulations *implicitly* include workers, they also rely on 'informed consent' as a basis for processing workers' personal data. However, as stated in the GDPR, informed consent cannot be freely given by workers in lieu of the power relations between management and workers[10].

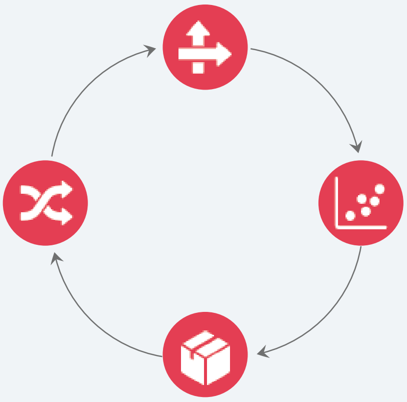
In addition, although employers in most data protections are obliged to *inform* workers of the data collected and the purposes of this collection, workers have no rights of consultation, redress, nor to edit or remove the data collected.

None fully fulfil the OHCHR principles., as described above.

Improving Workers' Data Rights

It is clear that worker's individual and collective data rights are poorly defined in the vast majority of countries and regions. The below depicts the Data Lifecycle at Work: from data collection, to analysis, to storage and offboarding it describes the topics that unions should be aware of and negotiate on as well as the rights workers should have. It leans on the 1997 ILO publication "Protection of workers' personal data. An ILO code of practice"[11].

The Data Lifecycle at Work



Data Collection:
Sources? Union access toand knowledge of? Rightsto refute/block?

Data Analysis:
Used in productivity & Human Resources.
What rights do workershave to access these data and theinsights/inferences drawn?
Can theyobject to these etc?
Unions should setredlines for what the data can be used for and what not

Data Storage:
Servers - where? Who has access? Under what jurisdiction?
Especially important due toWTO/ecommerce discussions

Data Offboarding:
Is data sold?
To whom? Deleted? Canworkers deny/ block who it is sold to?
This includes data sets, statistics, inferences

[8] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en
[9] https://secureprivacy.ai/blog/ab-25-what-this-ccpa-amendment-means-for-employers-and-employees
[10] See Article 29 Working Party Guidelines on consent under Regulation 2016/679, page 7. https://ec.europa.eu/newsroom/article29/redirection/document/51030
[11] https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

Some of the demands under each of the four stages, though far from all, are covered for workers in Europe's General Data Protection Regulation zone. For workers in most other jurisdictions, these rights—if negotiated—would be new.

Data Collection

The data-collection phase covers internal and external collection tools, the sources of the data, whether shop stewards and workers have been informed about the intended tools and whether they have the right to rebut or reject them. Much data extraction is hidden from the worker (or citizen) and management must be held accountable.

In the GDPR area, companies are obliged to conduct impact assessments (DPIAs) on the introduction of new technology likely to involve a high risk to others' information. They are also obliged to consult the workers[12]. Yet very few unions have access to, or even know about, these assessments—unions should claim their rights to be party to them.

Data Analysis

In the data-analysis phase, unions must cover the regulatory gaps which have been identified—namely the lack of rights with regards to the creation of profiles on workers using statistical probabilities based on the data collected. Whilst workers in the GDPR zone have a right to know which inferences are made using their personal data directly, they have no right to know about inferences they are subject to that do not include their personal data[13]. Such inferences can be used to determine an optimal scheduling, wages (if linked to performance metrics) or, in human resources, whom to hire, promote or fire. They can be used to predict behaviour based on historic patterns, emotional and/or activity data.

Access to the inferences is key to the empowerment of workers and indeed to human rights. Workers should have greater insight into, and access to, these inferences and rights to rectify, block or even delete them. Without these rights, there will be few checks and balances on management's use of algorithmic systems or on data-generated discrimination and bias.

Combined with the data collection phase, unions could here beneficially negotiate around the purposes of data collection and analysis. This includes determining the redlines for what the data collected can be used for, and what it can't.

Example:

The Teamsters in California have negotiated that location data from drivers collected to ensure their safety cannot be used in performance evaluations of said workers.

Data Storage

The data-storage phase is important, not least in relation to trade agreements and the negotiations over data flows. For example, e-commerce negotiations on the 'free flow of data', within, and on the fringes of, the World Trade Organization, aim to remove any nation's right to localise data within the territory of the nation. This could lead to data being moved to areas with lower privacy protection, which poses risks as workers' data could then be sold, rebundled, and sold again without having to adhere to the data protection policies of the country of origin

If data is allowed to flow freely across the world and workers have not secured much stronger data rights via national law or collective agreements, their access to and control over these data would be weaker still.

Data Offboarding

The last phase – data offboarding – is linked to the storage phase, but also relates to the possible selling of data/datasets that include workers' data. Unions must here be vigilant. This refers to the deletion of data but also the sale and transfer of data sets, with associated inferences and profiles, to third parties. Unions should be included in negotiations towards much better rights to know what is being off-boarded and to whom, with scope to object to or even block the process—this is hugely important in light of the e-commerce trade negotiations mentioned above. Equally, unions should, as a minimum, have the right to request that data sets and inferences on workers are deleted when their original purpose has been fulfilled, in line with the principle of data minimisation recognised in the GDPR (article 5.1c)[14].

[12] GDPR article 35 and ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 2/2017 on data processing at work
[13] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
[14] https://gdpr-info.eu/art-5-gdpr/

Example:

The financial sector union in Ireland has successfully negotiated two key articles in the staff policy in the bank – RBS. They are:

1. Anti-Commodification Clause
The Bank commits that it will not turn employee data into a commodity for sale or trade.

2. Respect and Human Rights
The Bank commits that it will not turn employee data into a commodity for sale or trade.
The Bank is committed to respecting workers' privacy and human rights as defined in law and in particular with regard to the UN's Universal Declaration of Human Rights and the ILO's 1997 Code of Practice on the Protection of Workers Personal Data.
See their press release here

Recommendations

To safeguard workers' rights in digitalised workplaces and prevent that oftentimes obscure data inferences and profiles shape the work opportunities of workers, unions should begin to negotiate for much improved data rights.

To successfully do so, unions could:

1. Train members and shop stewards on the role of data in digitalised workplaces and in society at large. This includes good advice on the use of employer-provided devices and good practices around safeguarding workers' privacy rights outside of working hours.

2. Consider establishing a cohort of digital shop stewards who are specialists in the datafication of work and workers. See also Brief 2.

3. Have union resources (legal experts, bargaining units and organisers) that can support the above negotiations.

4. Negotiate the data lifecycle at work from a human rights/workers' rights perspective and linked to that.

5. Create a union-wide data rights policy framework that can inform (digital) shop stewards in their negotiations. In line with human rights and the data lifecycle at work, this could include articles on:

a. General principle: Worker dignity and welfare in the use of data-driven technologies in the workplace should be ensured. Articles and standards should be established that give workers agency over new technologies, and that promote health and safety, protect the right to organize, and guard against discrimination and other negative impacts on workers.

b. Workers and/or their representatives should be party to all data impact assessments and the periodic reassessment of said.

c. Employers should provide notice to workers in a clear and accessible way regarding all data-driven technologies in the workplace. Notices should include an understandable description of the technology, the types of data being collected, the purposes of these systems and the rights and protections available to workers.

d. Data minimisation: Employers should only collect worker data when it is necessary and essential for workers to do their jobs. See also definition in GDPR https://gdpr-info.eu/art-5-gdpr/

e. Workers should have the right to access, correct, and download their data. They should receive all relevant information regarding that data, including why and how it was collected, if data inferences were made on that data and if so, what these are, whether the data was used to inform an employment-related decision, including hiring decisions. Employers should be responsible for correcting any inaccurate data.

f. Worker data should be safeguarded and protected from misuse. In particular, employers should not be allowed to sell or license/donate or otherwise give third parties access to the worker data; otherwise, the incentives to violate worker privacy by selling worker data for monetary gain are too high.

g. Individual workers' biometric and other health data should never be shared with third parties unless required by law.

h. Employers should only use monitoring and surveillance systems for narrow purposes that do not harm (directly or indirectly) workers.

i. Changes to monitoring and surveillance systems due to technological changes at the workplace should be subject to collective bargaining.

j. Data-driven technologies should not discriminate against workers based on protected characteristics such as gender, sex, age, disability, marriage and civil partnership status, pregnancy and maternity, race and religion or belief.

k. Removing protected characteristics from data-driven technologies should not automatically allow employers to bypass the other requirements in this policy framework. For example, many employers justify the selling or passing on of datasets that include workers' personal data by claiming that the datasets are anonymised and therefore cannot be linked to the individual workers. However, many studies show how relatively easy it is to de-anonymise datasets[15] thus putting workers' identity and privacy at risk.

6. Be cautious and critical to attempts at defining data as a commodity/asset. This includes suggestions to devise systems for the redistribution of the value-added of data back to the workers as a means of production. Rights should not be tradeable for money.

7. Consider ways to responsibly collect worker data to counterprove management's analysis (see brief 3), and thereby break the employer or system-led monopolisation of "truth".

[15] https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAImZ_o2Up5jda586F7I4qomlzWnAvy7a3pbaQ4D8vXb7WB3oxaA-ZMJHNpXWZM9W0uCR8aCSvyqd-ZGaCWrugvxJ_y7GYlwTuv5Cysn4MvhjGmLmVg4uLwMjspp5cT1epXQCMYLMgIpNIzUzEW_MIBPjNEQWiUrQ7tBOTr8VIFXU