TRAINING MATERIAL
Our Digital Future

For Digital Rights Organisers

Asia-Pacific - June 2021

Authored by:

Dr Christina J. Colclough, The Why Not Lab

& Susana Barria, PSI Asia Pacific

PSI

FRIEDRICH EBERT STIFTUNG

TRAINING MATERIAL: Our Digital Future

For Digital Rights Organisers

2021

Contents

Foreword

Digitalisation has been underway for some time blurring the boundaries and responsibilities between public and private actors from e-government and e-governance, education technologies, to public procurement outcomes, public infrastructure monitoring, to public workplace human resources. The digital transformation is, however, accelerating like never before across the world. It is likely to continue as the expected economic downturn in the wake of COVID-19 places pressure on public sector budgets for years to come.

In this environment, the risk is that governments across the world will not use these changes to provide better and more universal quality public services but to accelerate cost cutting, outsourcing and privatisation through the adoption of new technologies at the expense of users and workers. We must ask, how should we as workers in the public sector respond? How can we form and position our responses?

This training material will provide some of the key insights needed to build a coherent set of demands that will empower workers and hold public authorities to account in how and why they introduce disruptive technologies. The chapters mirror the workshops we will be holding and therefore can be helpful to read before each workshop. Chapter 1 provides an overview of some of the key digital transformations in public services and suggestions to union responses. Chapter 2 dives into the core of digital systems, namely to data and algorithms and the impact these have on workers' rights, democracy and quality public services. We end in chapter 3 by looking at models and methods for strong union responses on workers' data rights, the co-governance of algorithmic systems and an inventory of responsible digital tools that unions could benefit from to empower the workers' voice.

Chapter 1: Digitalisation of Public Services

Impact on employments, jobs, skills

Before we in the next chapters dive into what digital systems are and how unions can respond to these to safeguard diverse and inclusive labour markets, we will in this chapter be looking at the impact of digitalisation on public services, jobs, skills and worker autonomy – but in a different way.

Rather than focussing on the statistics for job losses or changes, and the well-rehearsed demand for more STEM specialists (STEM is short for Science, Technology, Engineering and Mathematics), we will be focussing on debunking myths and finding the gaps in the discourses that beneficially should be filed through union action.

We will be focussing on global developments as well as regionally specific ones. In the workshops we will, or have, drawn on examples and recommendations in the report: Digitalisation: A Union Action Guide for Public Services, Work and Workers. It is beneficial to navigate that report throughout the course.

Additional in-depth information on the effects of digitalisation by PSI sector and theme can be found in the following PSI reports:

1. Digital Trade Rules and Big Tech: Surrendering public good to private power
2. Digitalization and Public Services: a labour perspective

Digitalisation of Asia Pacific – an overview

In many countries in the region, the government is driving public digitalisation through policies that expand the role of the private sector, with important exceptions. Automation of government and administrative services is seen as a cost cutting strategy in line with a political understanding of small role of government. In addition, more technically advanced digitalisation is also seen by governments as an opportunity to attract Foreign Direct Investment, and as a “new engine of growth”. Government's role as facilitator of private expansion and profit can also extend to developing certain aspects of data infrastructure.

- In the **Philippines**, both automation of certain administrative services is outsourced to private companies as a cost cutting strategy. On the other hand,

the government is investing in setting up of integrated camera surveillance with facial recognition, including through a loan contracted from the Chinese state-owned company providing the technology for this project.

- In **India**, the government's Smart Cities Mission (SCM) covers the digitalisation and expansion of private participation in the provision of municipal water and electricity supply, solid waste management, urban mobility and transport, housing, IT connectivity and e-Governance (administrative services). It builds on and expands beyond previous urban renewal projects pushed by international financial institutions such as the World Bank and Asian Development Bank.
- In this narrative, **Singapore** and **Seoul** are taken as examples of successful smart city programmes in the region (Kang 2020).
- In **Korea**, healthcare is a key sector under the Industry 4.0 Strategy. It aims to cover healthcare big data systems, AI-based drug development, smart clinical trial systems, and smart medical devices. Interestingly, the public entity National Biobank of Korea is to store the data collected from various public health institutions. Creating the data infrastructure is seen as part of the government role to facilitate private sector growth. It is not clear if the data analysis will be supplied by a public IT company or by private one, though Samsung has entered into partnership with Microsoft's Azure to do just this.
- In **Indonesia**, the vertically integrated public electricity company PT PLN has digitalised the power sector with an intention to respond to two policy objectives: to decarbonise and to decentralise. In this process, smart meters are a step towards smart grids. The digitalisation process was in-sourced and data collection and direct user interface are internal company data, which are not readily shared. However, as a pilot project, General Electric was contracted to digitise power plants and use cloud-based software applications to analyse the data and smarten the grid in Bali.
- As way of exception, in **New Zealand**, the digitalisation of public libraries is led by the city council, and sometimes through networked hubs of local government. In this process, digitalisation is thought as an expansion of the social role of libraries and crafted to balance offering these new services but not losing face to face interaction. However, it is not known to us which companies have been contracted to develop the data platforms and if data analysis or maintenance is in sourced or outsourced.
- In **Nepal**, the government relied on not-for profit organisations to develop a phone application for counselling and monitoring of pregnant women in far-flung areas. However, both infrastructure issues (weak mobile network in villages and unreliable power supply in district headquarters) and lack of

engagement with the actors who were to use the applications (CHWs and local health facility staff) led to the failure of the program that has been discontinued.

Are public services digitalised? If so, in which sectors mainly, how and to what degree?

- **teleworking for (office based) public service workers** has increased across country groups during the pandemic, but might not stick in all countries to the same extent.
- **use of wearables/applications to do the work** (for surveillance and data collection) has been reported from Nepal for community health workers who are asked to enter the data on their door-to-door visits in a smart phone application. In India municipal service workers are asked to use wearables while preforming cleaning and other outdoor tasks. Wearables seem less used in OECD countries.
- **remote interactions with users** was already common, more widespread in Higher Income Countries (HIC) and city-states than in middle income countries (MICs). In Low- and Middle-Income Countries (L&MICs) administrative services have been moved online first, with some degree of automation as well as outsourcing of some digital functions. During the pandemic ***telemedicine*** has also increased to varying degrees, mostly in the private sector.
    - In Korea, a government-led pilot telemedicine trial between doctors and patients that run from July 2015 to February 2016, U-health, had failed as the sector was not ready. Remote treatment and telemedicine within the country requires amendment of Article 34 of the Medical Service Act, which does not have the guidelines for such practices.
- **Smart public service systems** is most seen in utilities and transport. Korea has an intelligent transport system and smart water quality system in Seoul. Indonesia has intelligent electricity network systems (around 50% of Indonesians use smart meters) and is developing smart grids (Open Gov Asia). Public safety in cities using integrated smart camera systems with facial recognition are integrated in smart cities' projects, or stand alone, such as in the Philippines.
- **Artificial intelligence in decision making** is the least advance and mostly limited to HICs. There were controversies in Australia with their use in social services. South Korea has developed AI-based clinical therapy for Alzheimer.

What are the key problems/challenges in relation to digitalisation in the region, for example, for workers, citizens, democracy, public service quality and access?

- Linkages with privatisation, either as private digital companies step in, or as digitalisation becomes part of a broader strategy to privatise a sector, or a broader trend of the nature of the private sector (as a more digitally savvy healthcare provider for instance).
- Implication for universal and equal access to services, considering the potential for cost escalation of digitalised services as well as the existing digital divides. Overcharging through submitting patients to unnecessary tests/analysis that use new digital technologies and collect data.
- Discrimination, gender or otherwise. In the health sector, patient discrimination by insurance companies. Victimisation of union members and leaders.
- Implications for traditional jobs as new tech-based work is created, intensification of workload linked to use of new technologies. This was raised by KHMU in context of Korea's health digitalisation. In Indonesia, the expansion of smart meters has displaced meter readers and bill collectors.
- Under-regulation of AI-based service provision, regulation of sharing of data, health data for instance. While there is often a stronger focus on individual data and privacy issues, it is also important to adequately regulate and govern collective or aggregate data.
- Misuse of data for surveillance and profiling of government critics, especially in countries where authoritarianism is in the rise.

Debunking Myths

Although almost all multilateral governmental organisations have “the future of work” as a priority area, only one– the International Labour Organisation – focusses (partially) on the impact of these futures *from* the workers’ perspective. Some speak about the impact *on* workers. When they do, workers become an object of study. Something different from the author or the authoring organisation. Mostly these studies speak of the consequences of automation on jobs. Very few question automation itself.

Left to fill the space in policy advocacy and awareness raising are the national, regional and global unions. No other body can, or should, take this role.

All Voices Are Heard

As a consequence, the emphasis in future(s) of work and in the digitalisation of work debates are generally not on workers' rights, including on equity, data rights and the necessary expansion of collective bargaining into digital issues. Whilst amazing research and activism is being conducted by people of colour and women, the dominant rhetoric is based on that of the privileged white man.

In an upcoming PSI report, current digitalisation-related clauses and guidelines affiliates are negotiating for are schematised in a taxonomy to help unions find inspiration, gaps and areas where further negotiation needs to be made. Currently, the majority of clauses and guidelines are concerned with:

a. Skills and lifelong learning
b. The right to be consulted on/informed about the introduction of new technologies, and to a lesser extent,
c. The right to disconnect.
d. This leaves some significant gaps – most of which are dealt with in this training material. The following table lists these gaps upfront.

Gaps in mainstream discourse on effects of digitalisation

- Workers' collective data rights;
- The co-governance of algorithmic systems;
- The obligation of employers to invest in workers' jobs and career paths when disruptive technologies are deployed;
- The regulation of what the acclaimed author Shoshana Zuboff calls 'markets in human futures' i.e. the rapidly growing trade in datasets and data inferences;
- The regulation of surveillance and monitoring systems in workplaces and stringent demands to limit their usage in respect of the Universal Declaration of Human Rights;
- Stringent demands on employers to be transparent around the systems they deploy;
- A nuanced and committed obligation to flush out and rectify bias and discrimination, and;

Regulation demanding transparent audits and impact assessments of these digital systems that include sections on social rights, human rights and workers' rights as an obligation.

The Robots Are Coming

Another understanding that has become mainstreamed is that technological developments and disruption are somehow inevitable. All of the job losses, changes, and consequences of digitalisation are *happening to us*. Not *by* us. As if digital forces are beyond human control and framing. This is a digital determinism that assumes that digital technologies are 1. Good, 2. Needed, and 3. Wanted. But are they?

This must be our first point of contestation. If we do not demand human responsibility and the regulation of these technologies, the disruption of labour markets and societies will be left unfettered in the hands of some of the world's most powerful companies.

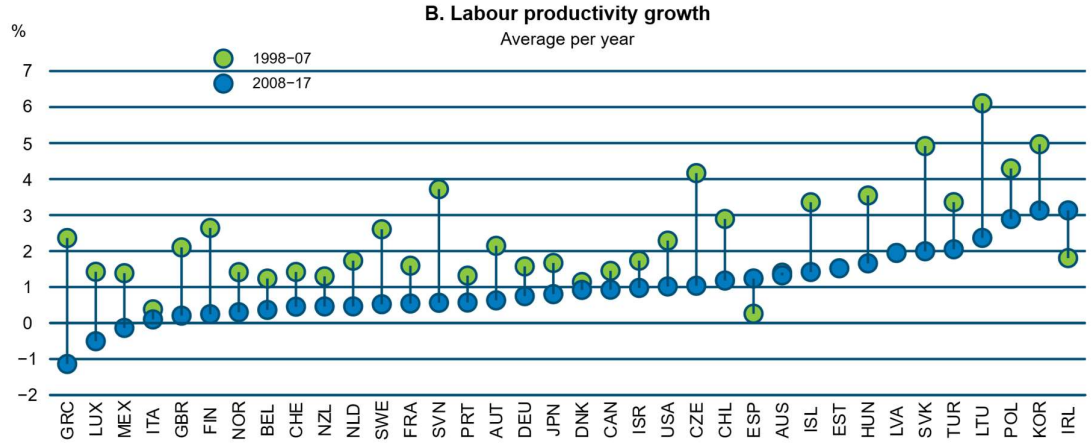
The realisation that algorithms and especially machine learning (see chapter 2) can self-learn and therefore ultimately have real-life consequences we do not know the background of, has pushed several governments to add "human-in-the-loop" or "human-in-control" wordings to their AI principles. Whilst this is good, it simply needs to be followed up by a union push for the regulation of these technologies. In chapter 3 we look at some of the policies unions beneficially could be pushing for. But key here is for unions to push for the regulation of all digital systems to ensure they put the interests and needs of people and planet before profit.

Digital Technologies = Productivity & Efficiency

Tech companies have succeeded in planting the narrative that digital technologies will boost productivity and increase efficiency. But do they? The systems might process lots of information fast. They might find interconnections the human brain would never do. But these are *system* efficiencies, not *impact* efficiencies. Do they really increase productivity if they are wrong? A cynical take would be that maybe the aim of a digital technology is to push workers to the breaking point to squeeze as much out of them whilst they can work, and then replace them. This is an efficient tool, but not – clearly – one that we as workers will support. So we must ask: efficient for what? For who? At what environmental, social, health cost?

There are many examples of algorithmic systems in the public and private sectors that have had adverse consequences requiring many many hours of human working hours to rectify. Every employer who claims their systems are productive or efficient, should be obliged to prove it.

Indeed, Organisation for Economic Cooperation and Development (OECD) research from 2019 shows that despite ongoing digitalisation, productivity growth has declined sharply across OECD countries over the past decades.



STEM Does It

Employers generally like to speak of the future of work as if it essentially is a debate around skills and especially STEM skills (STEM is short for Science, Technology, Engineering and Mathematics). This is a dangerous reduction of a complex, multifaceted change to work, workers, the social contract and rights.

Firstly, although the importance of STEM skills is undeniable, they too have their shortcomings. They simply cannot stand alone void of the humanities - social subjects, philosophy, anthropology, religious, economic and so forth skills. The current debates around AI Ethics proves the point.

Secondly, no system, be it a biological, economic or human system can survive if there is not sufficient diversity. The same goes for the labour market. We need workers with all sorts of skills and experiences, and a labour market that honours and respects the labour of workers no matter if they are in low-paid or high-paid jobs.

Blended/Hybrid Work - a Possible Future

Across the world, a cohort of workers have been working from home (WFH) due to COVID-19. Office spaces shut, commuter trains empty. Whilst WFH has been enabled by digital technologies, the mistrust many employers had towards their workers led to a sharp rise in the demand for employee surveillance and monitoring tools: from keystroke monitoring, to automatic screenshots of what websites and/or programmes were open on an employees screen, to the hijacking of webcams to

monitor the physical space and whereabouts of the workers. Yet note the change now in what employers are saying: from mistrusting the efficiency of remote workers, employers, as reported in the Washington Post on May 6, 2021 are now discussing to move employees out of employment and onto contract work.

This is a narrative that unions must play very close attention to also in regions of the world in which working from home has not been that prevalent. WFH has its merits, but although it is the privileged workers who could work from home, it potentially is also a route to the rising precariousness of work across these occupations. We must ask: A. what will happen to housing costs if WFH becomes the norm? They will rise, letting workers foot the bill and companies reap the benefits of much reduced office costs. B. What are the mental health costs of prolonged isolation? C. What will be the economic, social and mental health consequences of the potential end of the employment contract?

Outsourcing is Inevitable

As national budgets are expected to be under pressure for years to come due to the Covid pandemic, we can assume that outsourcing is going to rise significantly. This feeds well into the narrative that the private sector is far better resourced and suited to lead innovation that will make the public sector more productive and efficient.

Yet, a close look at outsourcing and service procurement regulations and guidelines across the world reveals that they do not include explicit mention of data obligations between the private actors and the public sector. This means that it is the private sector who holds all of the data and inferences derived from the procured task and services, and that the public sector therefore is at risk of not having access to these data and knowledge to actually perform their duties in the public interest. The risk of a corporate capture is all too real.

This will, unless changed, lead to a hollowing out of public services' ability to actually govern all whilst the private sector's power grab will rise. It is pertinent to raise awareness to this. On the long-term unions could table the demand of *joint data access and control* as a minimum in all outsourcing and service procurement agreements. Another possibility could be to demand transparency around the digital systems used both by public services and in procured tasks. Helsinki and Amsterdam do just this. as well as transparency around the agreements made between the two parties. Europe's Public Procurement directives are here helpful and should be replicated.

Management Understands

Another rather dangerous assumption is that local and central management actually understand the risks and challenges of the digital technologies they are deploying. This is far from the case. The examples we provide in chapter two: "Discrimination – disadvantaging the disadvantaged" clearly show that management did not have governance processes or structures in place to govern the impacts and outcomes of the algorithmic systems they were deploying. We must assume that had they understood the risks in these systems, they would much earlier in the process have governed and rectified the algorithms. The same applies in the context of smart cities. Here a key risk is that democratic bodies such as the local governments, will lose control/decision making power. This in turn will have dire implications for the ability of unions to bargain as the democratic spaces become irrelevant.

This is important. As unions capacity build and as you start pushing for the co-governance of digital technologies, many times management will be caught out. The same dynamic will most likely occur when workers and unions start demanding stronger data rights.

In workplaces and between managers, a new dynamic is arising between the tech departments and the human resource department. It is in that dynamic and the need for especially digital upskilling of human resource personnel that unions can get the upper hand.

Jobs are Created

We often hear that digitalisation is not lowering the number of jobs but is creating more new jobs. Politicians and especially employers celebrate this as a victory of the digital transformation.

However, in the Asia Pacific area which is home to 60% of the global workforce and the world's largest developing economies (Deloitte 2021), automation is predicted to be highly likely especially in labour-intensive sectors , but really across all sectors (see Figure 1 below). At the same time an ILO report from 2018 (ILO 2018) shows that 1.3 billion people work informally in Asia-Pacific, comprising 65 per cent of the world's informally employed. Most of them lack social protection, rights at work and decent working conditions.

The Asia-Pacific region is facing huge challenges that the celebrations of digitalisation and automation do little justice to.

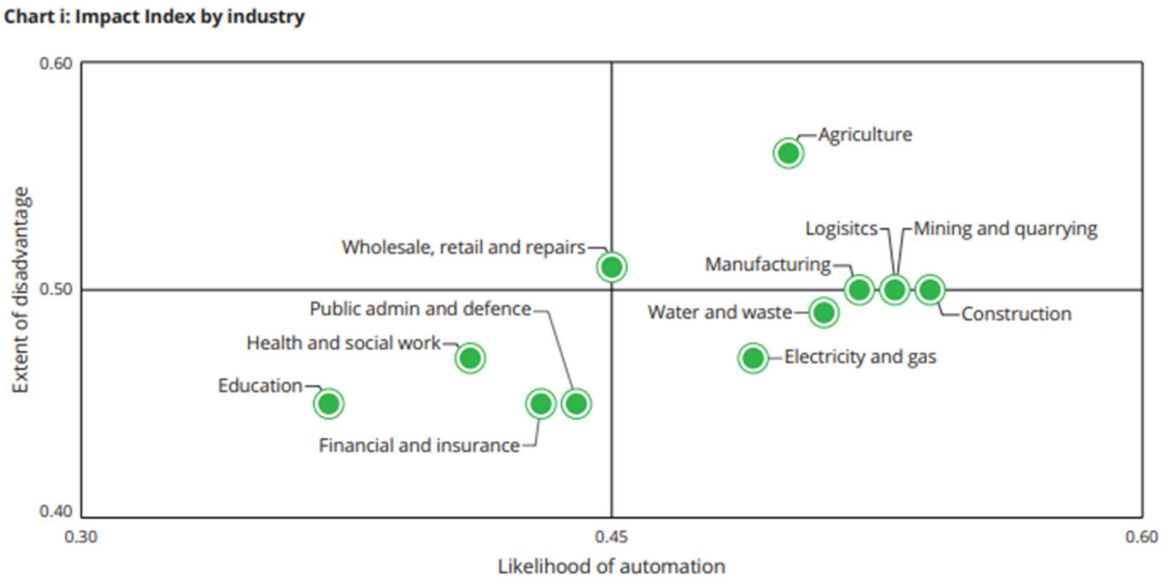


Figure 1: Likelihood of automation per sector APAC region (Deloitte 2021)

Summing Up

In this chapter, we have focussed exclusively on highlighting and problematising the dominant narratives around digitalisation. We have identified possible union push backs and suggested areas where unions should adopt a very critical interpretation of what is happening. This chapter lays the foundation for our critical assessments of all things digital that we will be dealing with in the chapters to come.

Chapter 2: Data & Algorithms

Impact on workers' rights, democracy and quality public services

In this chapter we will zoom in on all of this about data, AI and algorithms. We will define them and problematise them so we can better understand the impact of datafication on public services, work and workers and so we can be equipped to put union demands on the table.

Discrimination – disadvantaging the disadvantaged

Algorithms are fed data. These data can be real-life data or synthetic data. What numerous studies have shown is that the data is bias because we humans are. When fed into an algorithm, the outcome will therefore be discriminative. D'Ignazio and Klein in their epic book "Data Feminism" (2020) convincingly argue that the bias and discrimination in data and algorithms are a result of the unequal distributions of power. As most systems are designed by elite, straight, white, able-bodied men from the Global North, and most data analyses conducted by them too, the versions of reality we are fed, mirror the needs and wants of this dominant group.

We have numerous examples of this. Amazon who had to take down their automated hiring system as it only hired men. The UK Government who applied an algorithm to score graduate's exam papers, only to realise (too late) that it unfairly scored pupils from lower income neighbourhoods.

In the **Justice system** there is a wide-spread academic literature on the bias and discrimination inherent in algorithmic risk assessment tools. These tools are used in a variety of criminal justice decisions, assessing data such as an offender's criminal history, education, employment, drug use and mental health, then predicting the likelihood that that person will reoffend. The problem is, they disproportionately disadvantage people of colour. An example of this is Clearview AI - a highly criticised facial recognition tool used by law enforcement in 27 high income countries, including the U.S., France, Italy, the Netherlands, Norway, Sweden, and the United Kingdom.

AI is also used in **social benefits systems** across the world, often with little accuracy. For example, the Australian government has announced it will refund $720 million to

the almost 400,000 welfare recipients who were unjustly saddled with debt by a faulty algorithm. The automated welfare system nicknamed 'robodebt', pitted welfare recipients against faulty "income averaged" annual pay data. Lately, there has been a widespread withdrawal in the UK public sector from algorithmic systems used in benefit and welfare decisions.

UNESCO's recent report: Artificial intelligence and gender equality: key findings of UNESCO's Global Dialogue, states:

> *"Research, including UNESCO's 2019 report "I'd Blush if I Could: closing gender divides in digital skills through education", unambiguously shows that the gender biases found in AI training data sets, algorithms and devices have the potential of spreading and reinforcing harmful gender stereotypes. These gender biases risk further stigmatizing and marginalizing women on a global scale. Considering the increasing ubiquity of AI in our societies, such biases put women at risk of being left behind in all realms of economic, political and social life. They may even offset some of the considerable progress that countries have made towards gender equality in the recent past."*

As we will discuss in more detail in the next chapter, algorithms and data unarguably need governing. D'Ignazio and Klein recommend all deployers and analysts of data to ask a range of **"Who" questions** when questioning data and algorithms. Unions should demand that management answers the following questions and is held accountable for remedies and actions to ensure equity, equal treatment and quality public services:

> Who made this? Who collected the data? Whose lives are embodied in the data? Who is it serving? Who is potentially harmed?

A datafied world

The digitalisation of our work and societies has been long underway. In 1986, 1% of the world's information was stored in a digitised form. In 2007, it was 97%. Now it's 99.9%. However, all of this digitised information is not available for all to have insight

into, use, delete or share. Currently the US and China together account for 90 per cent of the market capitalisation value of the world's largest digital platforms, who in turn are those that control most of the digitalised information. These platforms in turn are superpowers dominating markets and societies. Microsoft, followed by Apple, Amazon, Google, Facebook, Tencent and Alibaba – account for two thirds of the total market value of all digital platforms.

For citizens across the world, data is being extracted from our actions and non-actions at a never-ending rate. Just think of your smartphone. It is a powerful computer that currently has 14 sensors in it. It follows your every step, as you (let's admit it) hardly go anywhere without it. It can show you the temperature, the route you should take, can connect you to the internet and all your friends. It can hear and see. It's powerful, it's handy, but it's also a surveillance apparatus like nothing else. It knows where you are. But also where you are not. It knows whether you exercise, how often, doing what? It also knows if you don't. It and the apps on it, are gathering data, making statistical inferences (profiles) on you, and using all of that for advertising, but also ultimately for manipulation. The world that is offered to you, the advertisements you see, are algorithmically determined. As the author of the renowned book "The Age of Surveillance Capitalism" Shoshana Zuboff recently said: "Once we searched Google, now Google searches us."

Add to that all the information you are sending out there when you use your credit card for what, or what you don't use it for. When you write something on social media, when you "like" a friend's post and don't like another, use government or private e-services of any kind, when you use your loyalty card to the shop or airmiles.

You are giving away data (information) that is used to profile and predict what type of consumer you are, what you most likely will vote, what type of worker you are, indeed who you are. These systems are obscure, hidden under the hood, surveilling you and predicting what you will do, should do, or what should be available to you and what shouldn't.

Think of all that data (picture it as a constant information flow you are knowingly or unknowingly giving away about yourself), and ask what influence it can, or might have, on your work and career? Maybe some of you have a LinkedIn profile. Now, data miners know your gender, age, what you do and don't do, and also what skills/education/work experience you have. It is not difficult to put a profile together on the type of worker you are: investable or less so?

It's Not Just About You

"*I've done nothing wrong, so who cares if they take my data?*" If you can hear yourself say this, you are not alone. The thing is: this is not just about you. Your data says a lot about you, yes. But it can have a huge impact on the work and life opportunities of people similar to you, or the absolute opposite. This is due to so-called "inferences" and the role they play in predictive analysis.

Statistics is the science of learning from experience, particularly experience that arrives a little bit at a time. Predictive analysis takes all the experiences extracted on your actions and non-actions, combines them with folks like you, or very different from you and churns this aggregated or collective data through powerful computational systems. The result is estimations on what you, and others like you or dissimilar to you, are likely to do in any given situation. Will your political affiliation change if you constantly are fed certain pieces of news – also fake news? Will your speed of work drop if you are working next to someone of this or that age, gender, or ethnicity? Will you buy organic food if you are shown certain advertisements? Will your bill be high or low if you get admitted to a private hospital? Research has shown that even when employers try to reach all audiences with a potential job advertisement, the audience is mediated by, for example, Facebook's algorithm. It is oftentimes *that* algorithm, rather than the employer's, that decides whether you are a likely candidate, and should see the job announcement or not.

Data at Work - Data is Power

Even in workplaces, the surveillance and monitoring of you as a worker that essentially creates data about you and what you do (and don't do) is information about you. That the employer knows whether you are talking to a colleague, or are going to the bathroom 5 times, or spending time by browsing the internet or taking a break, and how they then use this data is a question of power.

The employer and the systems they use are creating numerous "facts" about you and your colleagues that can have a real-life influence on your work life, employment continuity and career opportunities. Did they ever ask you for permission? Did they even inform you about these systems? Do you know what data is being extracted and for what purposes? Does the employer sell datasets to the many data brokers out there? If they do, have they told you that information derived from your actions and non-actions is an additional income stream? Where does all of this leave your privacy

rights? Is this changing the way services are provided by your team and to whose advantage?

A result of this surveillance society and labour market is the unequal distribution of power. If we as workers do not know what data is extracted, for what purposes, where it is stored, who has access to it, and whether it gets sold on, we are essentially disempowered. If we additionally have few, if any, rights to edit or block the data and the inferences derived from them, we are essentially being objectified. Turned into mathematical equations that either deem us to be productive, or effective or not so. The thing is, whatever the "result" be it horribly wrong, or worthy of an explanation, can have very harsh, very real impacts on our work life, job, careers and the services we contribute to provide. Similarly, the public services, as described in the Union Action Guide chapter 1, will too become commodified, void of a collective vision of social issues and problems towards a logic that attributes "risk" to the individual. This individualisation and risk-based approach is facilitated by data-driven inferencing, used in some countries in welfare benefit calculations, predictive policing and algorithmically defined exam grading.

This objectification, or as some call it, quantification of us, is turning labour – both the individual worker as well as us all as a collective sum of the parts – into a commodity. A tradeable asset that is void of our personality, dreams, thoughts and feelings

In an historical context, this current commodification of labour spurred by data and digital systems is particularly worrisome. In 1919, as part of the Treaty of Versailles that ended World War I, the International Labour Organisation (the ILO) was born out of the belief that universal and lasting peace can only be accomplished if it is based on social justice. The last sentence of Article 427 in the Treaty is shown in the box.

ARTICLE 427.
"…that labour should not be regarded merely as a commodity or article of commerce"

This article was reconfirmed by world leaders in the 1944 ILO Declaration of Philadelphia. Now as article 1a, it was stated:

> Labour is not a commodity;

The failure to protect workers' data rights in the datafied economy through adequate data protection and governance is nothing less than a governmental failure.

To overcome this and address the power asymmetries, we will present the Data Life Cycle at work in the next chapter and use this to discuss where and why unions must push for much stronger collective data rights in workplaces.

What is Data really?

In many legal texts (the European General Data Protection Regulation (GDPR) for example, or the Californian California Consumer Privacy Act (CCPA) and in some of the Asia Pacific countries (see table in Annex 2) , data is divided into two categories: 1. Personal data and personally identifiable data (Pii) and 2. Non-personal data, i.e. data that does not contain any information that can be used to identify a natural person. Most data protection regulations only cover data covered under item 1.

Some of the region's data protection laws cover "anonymised data", i.e. personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. However, as many experts argue, today, much economic value is derived from data that is not personal on its face but can be rendered personal if sufficient effort is put in place (Finck & Pallas 2020). This is really important for us to take note of. Anonymous datasets are really not that anonymous despite what the employers will say. We must ask whether the distinction between personal and non-personal data is a political one more than a realistic one. We must ask how workplace data that is not covered by data protection laws, can be used to negatively impact workers.

Data Protection regimes in Asia Pacific

According to an UNCTAD database, among the 60 countries of the Asia Pacific region, 57% have a legislation (lower than world average), another 10% a draft legislation (might not be updated), 27% have no legislation (higher than world average) and there is no data for 4 countries (including North Korea).

ASEAN has a Framework on Personal Data Protection that states principles for data protection with the aim to help ASEAN members in definition and implementation of domestic laws and regulations. There is no such framework under SAARC.

There are two countries in the region that are considered by the European Union to have data protection regulation at par with their own (called as GDPR adequacy), Japan and New Zealand (for an overview of relevant articles for workers in the GDPR, see Annex 1 – Benchmarking the GDPR). Thailand and Sri Lanka have legislations inspired by the GDPR. The Australian, Korean, Sri Lankan, and the upcoming Indian laws are considered to be strong on data protection.

Are workers included in the regulations?

Commonly yes. However, ***Singapore*** excludes employees in the course of their employment from the scope of the data protection law. ***Australia*** provides for conditional exemption, and in ***Thailand*** employers can collect and usie employees' data based on their "legitimate interest".

What is the legal basis for processing workers' data?

Contrary to the GDPR, where consent is insufficient as a legal basis for processing employee data, due to the power imbalances between management and employees, consent is the common legal basis for processing workers data in the region. Some legislations refer to express consent, informed consent, or define consent in a detailed manner. ***South Korea*** requires prior notification and opt-in consent (strictest). Non-sensitive data often only requires to be notified, rather than consent provided. See Annex 2 – Data Protection Asia Pacific for more specifics.

What rights do workers have?

	Australia	Singapore	Japan	Vietnam	Indonesia	Malaysia	India
Anonymity[1]	✓	×	×	×	×	×	×
Access	✓	✓	✓	✓	✓	✓	✓
Correction	✓	✓	✓	✓	✓	✓	✓
Confidentiality	×	×	×	✓	✓	×	✓
Data Breach Notification	✓	×	×	×	✓	×	✓
Data Portability	×	×	×	×	✓	×	✓
Data Quality	✓	✓	✓	×	✓	✓	✓
Deletion (if purpose served)	✓	×	✓	×	✓	✓	✓
Object to processing	×	×	✓	✓	×	✓	×
Object to marketing	✓	✓	×	×	×	✓	×
To be forgotten	×	×	×	×	✓	×	✓

Figure 2: from https://www.ikigailaw.com/data-governance-in-apac-findings/#_ftn6

Except when explicitly mentioned, workers have the same rights are other individuals under the country's data protection laws and regulations. Exceptions and exemptions are mentioned above. The table above lists some of the rights commonly provided under data regulations.

In Australia, employees personally identifiable data may only be processed if it is required for the performance of the employment contract and constitutes an

employee record. However, exemption from the application of Australia's data privacy laws is possible based on some criteria. Employee records are generally exempt, except for documents that pre-date the employment relationship (eg, pre-employment or hire documentation). At the time it collects personal information, the employer is required to provide the individual with a statement setting out the company's obligations under Australia's data privacy laws and the individual's rights. Further restrictions apply for sensitive personal data. Employee records – with the exception of tax file numbers – are not covered by the Australian notifiable data breach regime. Surveillance of employees is prohibited in sensitive areas, such as washrooms and change rooms, unless the surveillance device is installed pursuant to a warrant or authorization. Surveillance is permitted in public areas if it conforms with relevant legislation. The monitoring of an employee's use of a work computer (ie, emails and internet browsing) is governed by specific laws in some states (DLA Piper 2020).

In Sri Lanka, workers, like other data subjects, have the right to withdraw consent and object to processing of their personal data, to access personal data, to secure confirmation as to whether or not personal data concerning them is being processed by the entity they are in touch with, to rectify inaccurate or incomplete personal data, and to get personal data erased (IKIGAI Law 2019).

In India, the Information Technology Act, 2000 covers data protection and violation of personal privacy, including protection of employee's records. This statute safeguards against breaches in relation to data from computer systems and creates liability. It stipulates the penalty for breaches of confidentiality and privacy. Sensitive personal data or information is defined under the Sensitive Information Rules under the ITA to include passwords, financial information, physical, psychological and mental health conditions, sexual orientation, medical records and history, and biometric information. Any company receiving such information as a result of either using the services of an individual or employing an individual must comply with the Sensitive Information Rules regarding processing and storing such information. (DLA Piper 2020)

In Malaysia, employers must obtain employees' consent (implied or express) before collecting and processing employees' personal data, and explicit consent is required if "sensitive personal data" is being collected. Employers must notify their employees of the nature and purpose of information being collected, to whom it is being disclosed, and that the employees have the right to access such data. Employee

consent is also required before employee personal data is shared with third parties (for example, external payroll service providers). As a result of the PDPA, an employee consent/notice document is required. This document has to be bilingual – in both English and Bahasa Malaysia – and is usually a separate document and referenced in the employment contract (*ibid*).

In Philippines, when an employer collects and processes personal information of its employees, especially sensitive personal information, the employer must comply with applicable guidelines on the adoption of organizational, physical and technical security measures and the registration thereof with the National Privacy Commission. The data subject must have given their consent prior to the collection, or as soon as practicable and reasonable. An employer's collection of personal information from its own employees does not require the employee's prior written consent, provided the personal information collected and the processes applied to such information are only to the extent necessary for compliance with legal requirements prescribed for an employer-employee relationship (*ibid)*.

In Singapore, employers are required to notify applicants of the purposes for which their personal data is being used in connection with the management and termination of employment and/or obtain their consent where collecting, using or disclosing their personal data. However, an employer is permitted to collect, use and disclose the employees' personal data for purposes of managing or terminating an employment relationship without the need to seek employee's consent. Employers may collect, use and disclose personal data without obtaining the employees' consent or notifying them where it is necessary for evaluative purposes, including the determination of the suitability or eligibility of an individual for employment, continuance in employment or promotion. Employers must seek consent for purposes that are not related to the employment relationship unless any other exception under the PDP applies (DLA Piper 2021.

In New Zealand, the same data subject rights apply in respect of employees (e.g. access to, or correction of, personal information) than other individuals. There are additional requirements for processing information relating to employees or employment. A lawful purpose is required as with other personal information, and employers can only collect personal information about employees for valid work-related purposes, or where directed to by law (OneTrust Data Guidance).

In South Korea, under the PIPA, an employee is entitled to request the employer to allow access to, correct or delete their personal information. The PIPA requires an

employer to obtain the consent of the individual employee when their personal information is obtained or provided to third parties.

What's all this about algorithms and AI?

98% of Fortune 500 companies use AI or data driven systems at some stage of their hiring process, and this is spreading. The coronavirus crisis is accelerating the adoption of such automated decision-making systems to recruit, evaluate, track and onboard employees. Employers are 'panic-buying' automated onboarding and monitoring systems. Amazon, for instance, recently used data-driven technology to on-board 1,700 staff in a day. Serco, a private provider of public services across the world, has cut the time it takes to hire a worker from 4 weeks to 4 days.

Automated hiring systems, scheduling tools, worker monitoring, GPS tracking, keyboard click speed measuring are only but a few of the algorithmic systems being deployed by public services and private companies alike. To better understand how workers can protect their autonomy and prevent the commodification of their labour, it is important we spend a few moments unpacking the concepts of algorithms, artificial intelligence and machine learning. The next sections will be all about that.

Algorithms

There are many terms that describe the inner workings of digital systems. At the core of all digital systems are algorithms. Algorithms are a series of mathematical operations: equations, algebra, logic, probability, calculus that are translated into computer code. This code is then fed with data, some of this data is from the real world (for example, information about your whereabouts throughout the workday), other data is "synthetic" – data that simulates the real world.

Definition of an Algorithm:

"A step-by-step procedure for solving a problem or accomplishing some end especially by a computer."

(Fry, 2018)

Algorithms are a series of instructions that show from start to finish how to accomplish a task or solve a problem. Think of an algorithm as a recipe. The algorithm is tasked to make the best tomato soup. It is *instructed* to cut 200 grams of onions, fry them off, add the garlic, then use 2 cans of tinned tomatoes. The result of the algorithm will be very different if you change the order of the instructions, for

example if you fried the tomatoes and not the onions. So, what counts here is the **1. instructions** and **2. the order of those instructions.**

Hannah Fry (2018) helpfully list four different categories of algorithms:

Prioritising Making an ordered list	You know these from your Facebook news feed - what posts do you see, which don't you? Or your Netflix or Spotify recommendations. Ordered lists use a mathematical process to order all possible choices and return to you what it seems "best" or "fastest" etc. Think of the route recommendations you get when you ask your map app how to get from A to B
Classifying/ Profiling Putting things in boxes	No matter what you do online, you are being classified/profiled. A student, a nurse, an engineer. A man, a woman. A union member. You get classified by algorithms as someone most likely interested in what advertisers want to sell you. Baby clothes if you are a woman in your early 30s. Cars if you are a man in your 40s. The stereotyping is clear. And effective. These algorithms also remove contents they don't think you would want. Classification/profiling algorithms are highly manipulative.
Associating Find Links	Dating apps run on associating algorithms. Matching folks to one another through connections of one kind or another. Amazon and other e-commerce sites also run association algorithms. Have you ever seen the "Other customers also bought x, y or z" message? Or the "People who bought this item also looked at this one"? These are association algorithms. Association algorithms can be horribly wrong as we have seen in discriminative predictive policing algorithms or credit scoring systems.
Filtering Isolating what's important	Siri, Alexa, Cortana and every other digital system you can talk to are speech recognition algorithms. They are designed to filter out "noise" and focus on what they think you, and not someone in the room with you, are saying that is important. Facial recognition works in the same way. These systems can classify words/traits they don't recognise and filter accents/faces they are not trained on as noise. Minority workers in call centres have felt the discrimination in these systems all too clearly.

Most digital systems use a combination of the above 4 categories. For example, if previous profiling systems have shown that women are perceived as more trustworthy homecare workers than men (*classifying/profiling*), and that a male homecare worker is most likely to find another job if he is asked to work early hours (*associating*), than the likelihood that a male applicant for an early morning homecare job will be called for an interview is low.

All algorithmic systems that inform real-life decisions we call Algorithmic Decision-Making Systems (ADMs).

Summing up, as we aim towards ensuring diverse and inclusive employment in the public sector, and ensuring quality public services we need to ask into:

1. The types of algorithms
2. The order of instructions
3. The data used to train or maintain the algorithm.
4. The purpose and aim of the ADM

For our quest **to ensure quality public services** that are fair and equitable these questions are equally important. As we discussed in chapter 1, we can expect more functions within public services to be outsourced or data related services procured because of the Covid pandemic and large public debts. If the contracts between public services and the private sector do not include 1. Joint oversight over algorithmic systems deployed and 2. As a minimum joint data access and control, the public services will lose oversight over how conclusions in the public interest are drawn, and they will lose the means to govern (the information) in the public interest.

In chapter 3, we will discuss a couple of practical models for "negotiating the algorithm", but for now, let's continue unwrapping the link between algorithms/ADMs, artificial intelligence and machine learning.

Artificial Intelligence & Machine Learning

AI is a scientific discipline, like mathematics or biology. This means that AI is a collection of concepts, problems, and methods for solving them.

Although the definitions of A.I. vary, most of what is called Artificial Intelligence (A.I) is actually **rule-based algorithms.** These are algorithms that have received direct and unambiguous instructions from a human. Let's take our recipe example again. A rule-

based algorithm has been instructed to make tomato soup. It has been told to 1. Fry 150g of onions, then 2. Add 2 sliced garlic cloves, then 3. Add 400 grams of tomatoes, etc. Rule-based algorithms follow the structure of "if this – then that". *If* you have fried the onions and garlic, *then* add the tomatoes.

Rule-based algorithms can be immensely powerful. In a worker evaluation system, the instructions can be: 1. If a worker is slower than the norm at his or her tasks and has been for over 2 months, then call him or her to a formal meeting to discuss their performance and contract. Or more complexly: If the worker shares 80% similar features to the group of workers we previously have identified as less productive, and is a union member, then fire immediately. The power lies in the instructions as well as in the outcome and the effect it has on workers. For our quest to ensure inclusive and diverse labour markets, quality jobs and quality public services, we must be party to the governance of these algorithms.

Machine Learning

> ***Definition of Machine learning***
>
> *"the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data."* Arthur Samuel, 1959.

Machine Learning is a subset of artificial intelligence. Machine learning is the process that powers many of the digital services we use today—recommendation systems like those on Netflix, YouTube, and Spotify; search engines like Google and Baidu; social-media feeds like Facebook and Twitter; voice assistants like Siri and Alexa.

In machine learning there are no clear instructions to the algorithm. You give it data, a goal and feedback when it's on the right track, and **it will learn by itself** how to cook the best tomato soup. *How* it makes the soup is somewhat of a mystery – hidden oftentimes in the "black box" of the algorithm, the lack of instructions means we, at least in principle, have little control over the process.

In the example of the soup, we do not know in what order it put the ingredients. In our world of work, we will not know how the machine-learning algorithm arrived at the decision to recommend Mary to the job over all other candidates. Is the algorithm respecting anti-discrimination laws? Has it chosen Mary because of some obscure fact about her that no other candidate exhibited? Did it compare Mary's CV with job seekers from another sector, country or region of the world but not the other candidates?

Machine Learning algorithms improve automatically through experience or historical data. For example, you did not hire Mary as it turned out she wasn't interested in working on the tasks at hand, but rather hoped to get her foot in the door and from there transfer over to her "dream" job. You added this information to your database, that then gets added to the algorithm and next time it is used to pick a good candidate or two, it will automatically look for signals of "loyalty", "tenure" or whatever else it finds correlates to "genuine interest in the job".

Currently, machine learning has been used in multiple fields and industries. For example, medical diagnosis, image processing (including facial or emotional recognition), prediction (including predictions on crime, fraud, child neglect, worker disloyalty or organising efforts), classification (for example good/bad worker), learning association and regression (predicting the price of labour based on the features of that labour - for example, gender, age, education, location, supply of similar labour and so forth).

We must ensure quality jobs that respect human rights and workers' rights and that are governed fairly without opaque discrimination and algorithmic harms. We strive quality public services and inclusive and diverse labour markets. Machine learning algorithms are a threat against this. Especially the claim they are difficult to govern as we do not have access to the process is a huge concern. In the next chapter, we will discuss what unions should respond when they are told by management that "they simply don't know".

Summary of chapter

In this chapter we have learnt that the datafication of work and workers is leading to a bias, discriminative and unequal distribution of power that disfavours the already disadvantaged. All digital technologies embed cultural, normative and/or valuative legacies be they integrated through the data sets an algorithm is trained on with all of the bias and discriminations these contain or be it through the instructions to the

algorithm. No data system will ever be "fair" if it is not governed. In addition, algorithmic systems can be designed and trained to reduce costs (financial costs) and increase revenues from paid public services rather than improve the quality of these services.

We have discussed what data and algorithms are and the various typologies of these. We can use this knowledge when we start questioning management on their use of algorithmic decision-making systems. We have also shown examples of the negative impact of ungoverned algorithmic systems in the public and private sectors.

With this knowledge, we will now turn to the next chapter which presents methods and models for dealing with all of this through collective bargaining and/or law so we can empower workers and prevent the irreversible commodification of work and workers.

Dig Deeper - good resources

Books	Veliz, Carissa (2020): **Privacy is Power**, MIT Press
	D'Ignazio & Klein (2020): **Data Feminism**, MIT Press
	Fry, Hannah (2018): **Hello World – Being human in the age of algorithms**. W. W. Norton.
	Eubanks, V. (2018) **Automating Inequality**. New York: St Martin's Press.
	O'Neill, C. (2016) **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. London: Penguin.
	Ruha, B (2019): **Race After Technology: Abolitionist Tools for the New Jim Code**. Wiley
Articles/reports	Sánchez-monedero, J., & Dencik, L. (2019), **The Datafication of the Workplace** https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-The-datafication-of-the-workplace.pdf
	Access Now (2021): **DATA MINIMIZATION: KEY TO PROTECTING PRIVACY AND REDUCING HARM** https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf

	Data Privacy Laws in South East Asia: https://blog.mithi.com/data-privacy-laws-in-south-east-asia/
	Data protection regulation in South Asia, December 2019, https://www.ikigailaw.com/new-era-of-data-protection-regulation-in-south-asia/#acceptLicense
	Introduction to Digital Security Laws in Nepal, Sri Lanka, and Bangladesh, Aug 2019: https://www.ikigailaw.com/introduction-to-digital-security-laws-in-nepal-sri-lanka-and-bangladesh/
	Employment and Data Privacy: https://www.dlapiperintelligence.com/goingglobal/employment/index.html?t=11-data-privacy
	Noble, S & Robert, S (2019) **Technological Elites, the Meritocracy, and Postracial Myths in Silicon Valley**. Available here: https://escholarship.org/uc/item/7z3629nh
	Bogen, M., & Rieke, A. (2018). **Help wanted: An examination of hiring algorithms, equity, and bias.** Washington, D.C. Retrieved from https://www.upturn.org/reports/2018/hiring-algorithms/
	Kresge, L. (2020). **Data and Algorithms in the Workplace: A Primer on New Technologies**. Retrieved from https://laborcenter.berkeley.edu/working-paper-data-and-algorithms-in-the-workplace-a-primer-on-new-technologies/
	Adler-Bell, S., & Miller, M. (2018). **The Datafication of Employment.** The Century Foundation. Retrieved from https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/
	Moore, P. V. (2020). **Artificial intelligence in the workplace: What is at stake for workers**? In Work in the Age of Data (pp. 1–14). Madrid: BBVA. Retrieved from https://www.bbvaopenmind.com/wp-content/uploads/2020/02/BBVA-OpenMind-Phoebe-V-Moore-Artificial-Intelligence-in-workplace-what-is-at-stake-for-workers.pdf
	Metcalf et al (2021): **Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts**, retrieved from: https://dl.acm.org/doi/pdf/10.1145/3442188.3445935
	Ada Lovelace (2020): **Examining the Black Box: Tools for assessing algorithmic systems**, retrieved from:

	https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/
	Ada Lovelace (2020): **Transparency mechanisms for UK public-sector algorithmic decision-making systems**, retrieved from: https://www.adalovelaceinstitute.org/report/transparency-mechanisms-for-uk-public-sector-algorithmic-decision-making-systems/
	Sloane, Mona (2021) **The Algorithmic Auditing Trap**, retrieved from: https://onezero.medium.com/the-algorithmic-auditing-trap-9a6f2d4d461d
	Colclough, C: (2020): **Workers' rights: negotiating and co-governing digital systems at work**, retrieved from: https://www.socialeurope.eu/workers-rights-negotiating-and-co-governing-digital-systems-at-work
	Brione, P. (2020) My Boss the Algorithm: an Ethical Look at Algorithms in the Workplace. (Acas Research Paper)
	West, S.M., Whittaker, M. and Crawford, K. (2019) **Discriminating Systems: Gender, Race and Power in AI**. New York: AI Now Institute. Retrieved from: https://ainowinstitute.org/discriminatingsystems.html
	McKinsey (2018) https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-in-black-america
Websites	http://gendershades.org/
Courses	https://www.elementsofai.com/ The Elements of AI is a series of free online courses created by Reaktor and the University of Helsinki. Highly recommendable.
Newsletters	The Mark Up: https://themarkup.org/
	The Ada Lovelace Institute: https://adalovelaceinstitute.us1.list-manage.com/subscribe?u=7614620d1284fd7ff1c97d04d&id=fdd10eabe7
	Data & Society https://datasociety.net/research/labor_futures/
	AI Now Institute: https://ainowinstitute.org/

Chapter 3: Empowered Workers and Quality Public Services

This chapter builds on the two first and offers concrete strategies and policies that unions could be pushing for in law, regulation and/or collective bargaining to empower workers and public services. It will give ideas and inspiration for negotiations on workers' collective data rights, public services' data access and control, the co-governance of algorithmic systems, just transition policies and lastly it will provide examples of how unions can use *tech for good* to empower workers.

Workers' collective data rights

As we discussed in the previous chapters, data is being extracted, analysed, inferred, and maybe even sold or reused at an increasing pace. Whilst workers in the European Union have some useful data rights secured through the General Data Protection Regulation (GDPR), this is less the case in the Asia Pacific region..

Improving Data Rights - Negotiating the Data Life Cycle at Work

Despite the helpful protections in the GDPR for workers, there are also real gaps. Spain addresses a couple of these in a new royal decree-law, which is the first of its kind in Europe. It has an article and two final provisions, the purpose of which is to specify the right to information of the representation of workers in the digitized work environment, as well as the regulation of the employment relationship in the field of digital delivery platforms. It says:

> "The Workers Council of any company shall have the right, periodically, as may be appropriate, to:
>
> Be informed by the company of the parameters, rules, and instructions on which algorithms or artificial intelligence systems that affect any decision-making that may have an impact on working conditions, access to and maintenance of employment are based, including profiling."

This is a wonderful development which addresses some of our concerns raised in chapter 2. For all workers inside and outside of the GDPR, it is helpful to consider how workers' collective data rights can be additionally improved across what we call the Data Life Cycle at Work.

As we discussed in the previous chapter, algorithms are fed real life data or synthetic data. The majority still rely on real life data. This means that there is some form of **data input.** This data can be obtained through historical accounts, such as previous hires or data sets that are bought from third parties, such as census data, labour statistics, educational data, election data and much more. It can be combined with contemporary data for example from monitoring and surveillance systems at work and social media accounts.

The **data is then used, analysed and inferred**. Here the four types of algorithms we identified in chapter 2 are helpful to understand what some of these inferences could be. If the algorithmic decision-making system is an automated hiring tool, the inferences can be obtained through classifying and associating algorithmic systems. The system might, for example, find links between loyalty levels, postcode, educational level and gender.

Then the **data is stored** somewhere. The Cloud is not void of geographical location. The data can be stored on servers in your jurisdiction or elsewhere. Knowing where is important for determining who has the right of access to the data.

Lastly **data can be off-boarded**. They can be deleted or sold as bundles of anonymised inferences or data sets.

The figure below depicts the Data Life Cycle at Work and lists questions unions should ask management to empower workers.

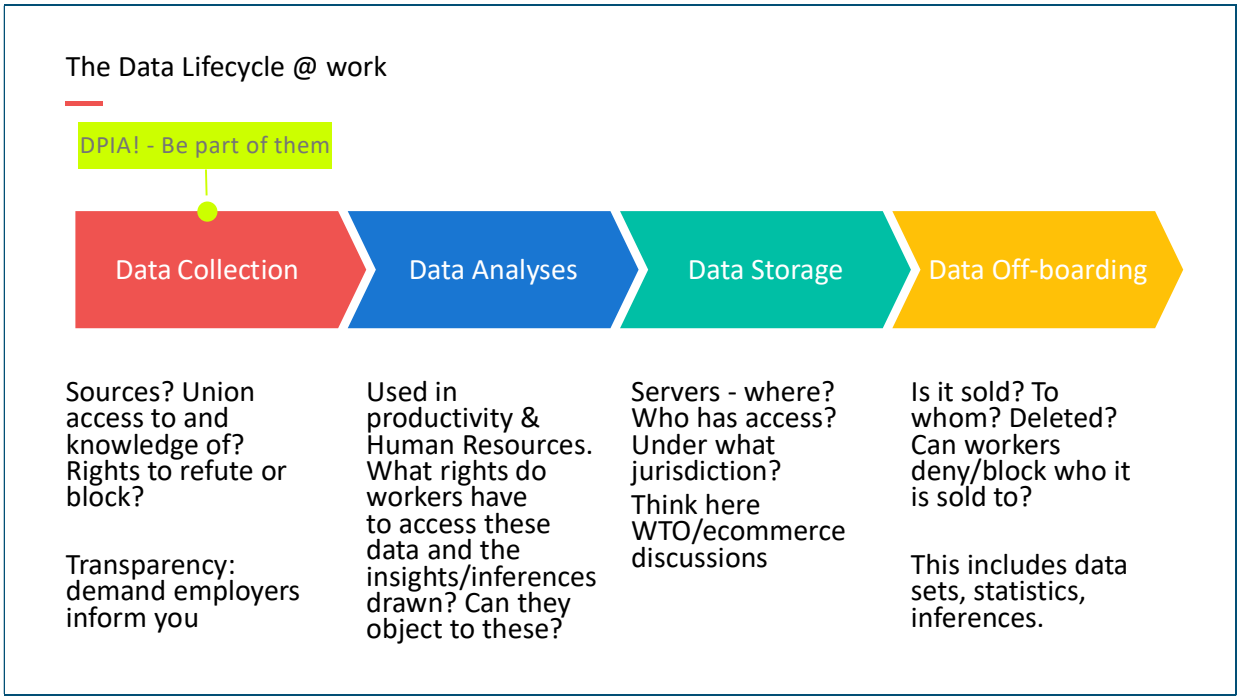


Figure 3: The Data Lifecyle at Work

Co-governing Algorithmic Systems

holding public services and management accountable

In this section we will look at some of the demands unions should table to hold public services and employers accountable to the algorithmic systems they put in place. This will not only be a benefit for public service workers, but also to prevent harms to our communities.

Transparency requirements

The first and essential demand must be to require that public services are transparent around which algorithmic systems they are deploying as part of their services towards citizens, but also workers.

A Finnish start-up on responsible AI, Saidot, is working with public authorities to do precisely that. Helsinki, Amsterdam and Nance have signed up. Saidot is currently in negotiation with the UK government for them to join the system too. A caveat is that public authorities are not required to be transparent around systems aimed at ensuring public safety. This unfortunately covers all public sector CCTV, facial recognition systems and policing. That aside, the idea is good.

Many shop stewards and unions report that they simply do not know what systems are being deployed. Interestingly, ILO Convention no 94 from 1949, which has been ratified by 63 countries actually demands that public authorities consult with shop stewards on procurement or contracts regarding "the performance or supply of services". Had this convention been respected, many more would know.

From data use to governing algorithms

If unions succeed in making management far more accountable and transparent around their data use, we have taking the first important steps towards governing algorithmic systems.

Let's recall the good "who" questions as suggested by D'Ignazio and Klein (2020):

> Who made this system?
>
> Who collected the data?
>
> Whose lives are embodied in the data?
>
> Who is the system serving?
>
> Who is potentially harmed?

These questions are essential for unpacking the potential discriminations and bias in algorithmic systems; however, they are not enough. We need to supplement them with, *at least*, the following:

1. Which systems are management using that relate to workers? This question aims to unravel not only the overall purpose of the system (for example automated hiring), but also the algorithms that constitute them (refer here back to Hannah Fry's classification in chapter 2).
2. Who owns these systems?
3. What are the contractual arrangements around data access and control?
4. Who is accountable and responsible for these systems?
5. What governance mechanisms does management have in place?
6. What remedies are in place if a system fails its objectives and/or if management fails to govern the algorithmic system?
7. What assessments have you made in relation to risks/impacts on workers' fundamental rights and privacy rights?
8. How do you control for, monitor possible discrimination and bias in the systems?

9. Do you periodically reassess the systems for unintended affects/impacts?
10. What are the mechanisms and procedures for amending the algorithmic systems?
11. How does this impact on the services we are providing?
12. Do you log your assessments and adjustments?
13. Who decides all of this?
14. What mechanisms can we put in place, so we are party to this governance?

Ideally, shop stewards would be co-governing these systems. In Europe, some countries already have works' councils or co-determination structures in place that could offer the space for this co-governance. In Norway, the 30-year old right for unions to have a "Data Shop Steward" could form the basis for it.

In all countries, the aim should be to establish co-governance bodies through collective agreements and/or law. In the meantime, posing the questions above to management is an essential first step.

A model for governing algorithmic systems could look like this:

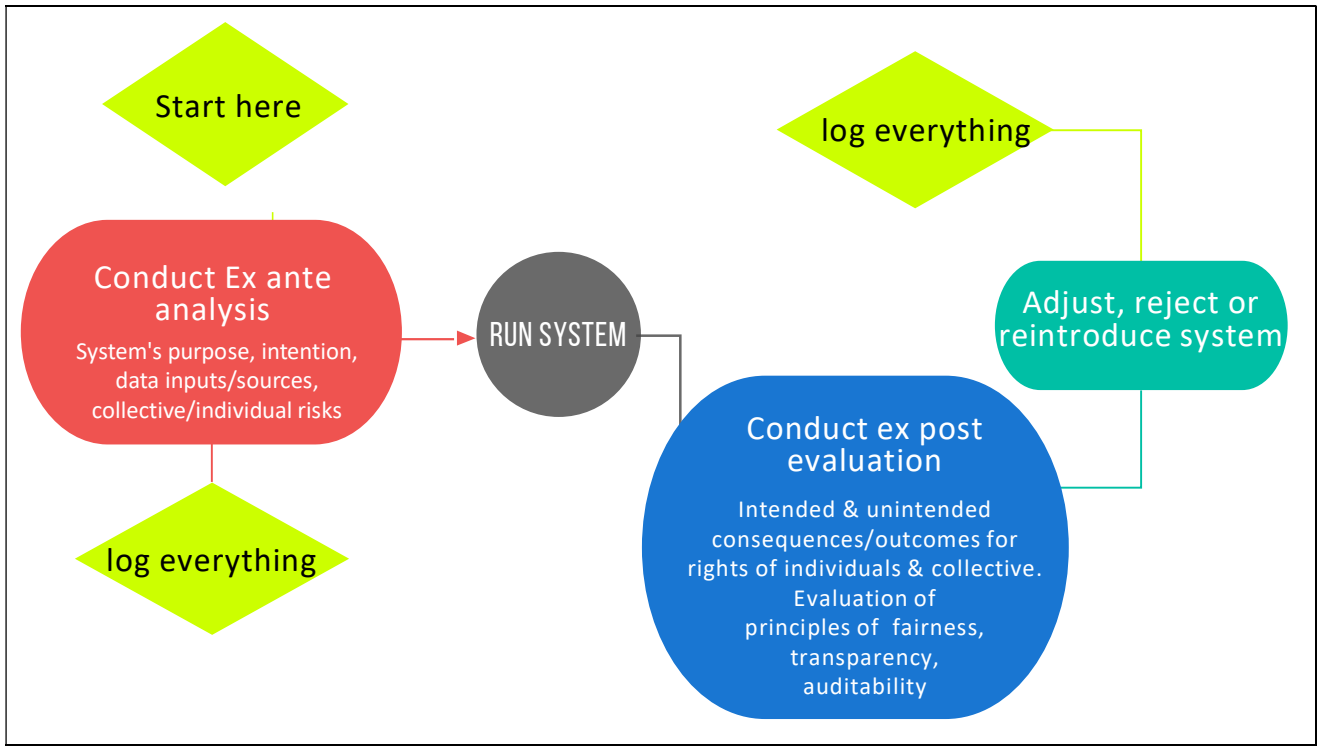


Figure 4: A model for co-governing algorithmic systems

What is particularly essential in this model is the **ex-post periodic re-evaluation of all algorithmic systems**. This phase is often omitted in governance models as you will

see in the Canadian government example below. As we learnt in chapter 2, machine-learning systems automatically learn. They can learn to be horribly wrong, disfavour certain population groups and prioritise others. Many of the scandals in public services' use of algorithmic systems could have been discovered and avoided had governance mechanisms been in place.

To allow unions and the public services to keep a check and balance on the impacts of these systems, it is important that the ex-ante and ex-post assessments and evaluations are logged and filed. So should any adjustments to the systems on the basis of these assessments. It is difficult to find patterns of discrimination or other forms of adverse effects if the impact assessments, audits and adjustments are not written down. Whilst it is important for unions to aim to be party to the governance of algorithmic systems, the responsibility for their deployment and impacts must always be the employers.

Lastly, it should be made very clear what the consequences of harm to others are. For example, public services should be demanded to explicitly inform users and workers alike of their rights, and also what fines, penalties and/or court proceedings can be issued when harm has been done. The rectification of harmful systems must be made public.

An example from the Canadian government

The Canadian government has introduced an Algorithmic Impact Assessment (AIA) in the form of questionnaire that determines the impact level of an automated decision-system.

The tool was developed to help organizations "better understand and mitigate the risks associated with Automated Decision-Making (ADM)."

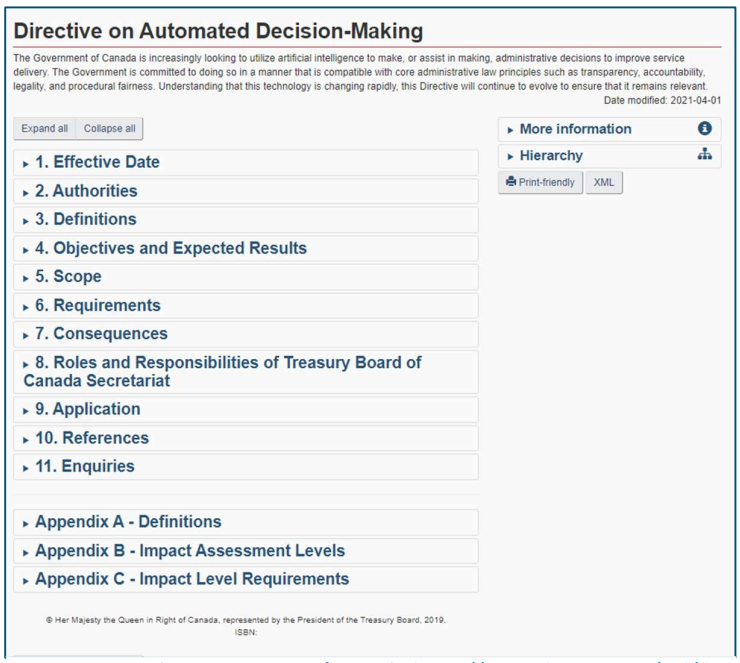


Figure 5: From the Government of Canada https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

It is composed of 48 risk and 33 mitigation questions. Assessment scores are based on many factors including systems design, algorithm, decision type, impact and data.

Whilst a very positive initiative, the AIA has some considerable deficiencies. The AIA is not required to be revisited periodically. Workers are not mentioned as actors.

The People Plan - Disruption's obligations

The union movement spearheaded by the ITUC has been pushing for Just Transition policies for workers whose jobs are disrupted because of a transition to a low carbon world. We can draw inspiration from that, and demand that employers who invest in disruptive technologies that will have an influence of workers' jobs and tasks should be met with a number of obligations. In the "People Plan" they should:

a. Map with the shop stewards the current workers' skill profiles;
b. Determine with the shop stewards and trade unions the re- and upskilling needs;
c. Offer courses **in working time**, as part of working time;
d. For displaced workers, co-develop with the worker and his or hers representatives a career development plan;
e. Work with employment agencies and other companies to help the individual onwards, and;
f. Apply these obligations throughout the supply/value chain affected.

Tech for Good

The last section in this chapter is about unions tapping into the power of digital technologies but doing so responsible and with the privacy of their members at the core of all digital activities.

In **Connective Action** – a report from 2019, a number of digital tools built for, or by trade unions, are presented together with a list of recommended apps and tools for union organising and campaigning. This report was writing by the team behind the Young Worker's Lab (YWL) – a pop up participatory action research lab at UNI Global Union.

WeClock

The YWL also produced an open-source app called **WeClock**. It works by tapping into the data that some of the 14 sensors on a mobile phone produce and gives the worker full control over that data. There is no third-party data snooping, no secret access.

WeClock is designed to help workers and their unions combat wage theft and promote worker wellbeing.

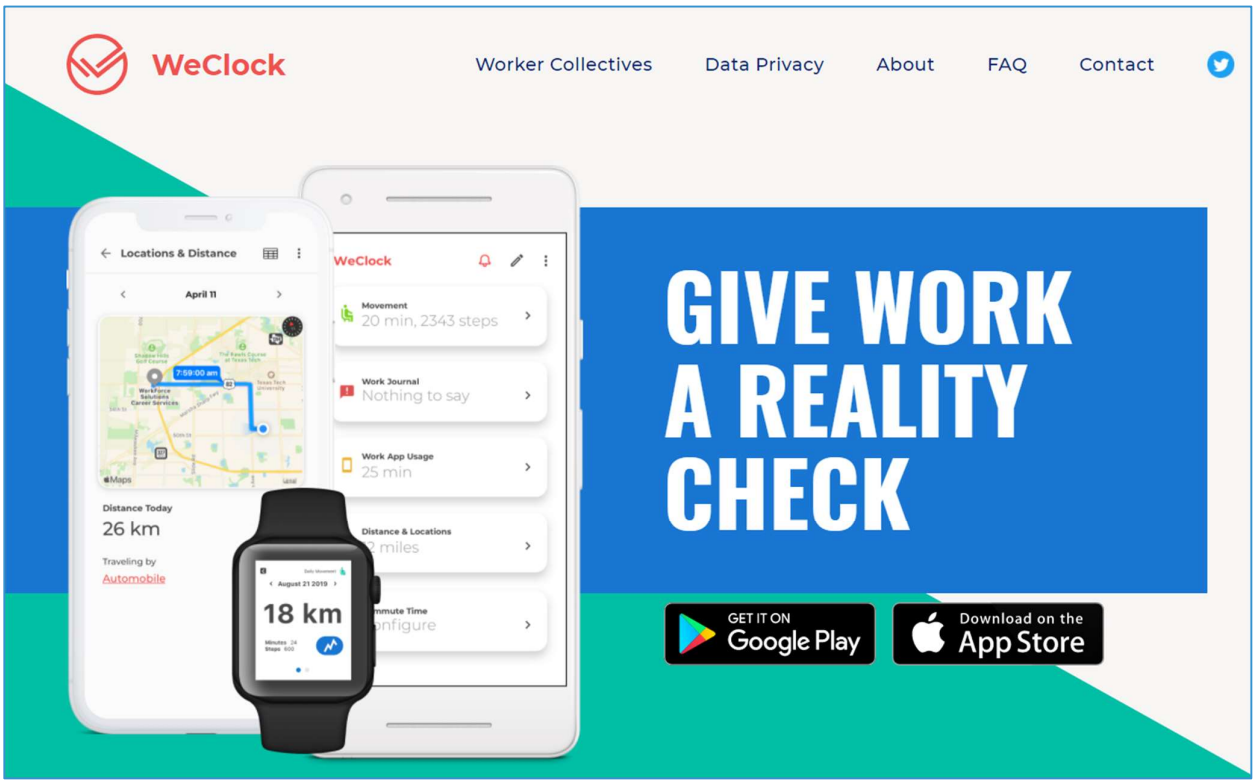
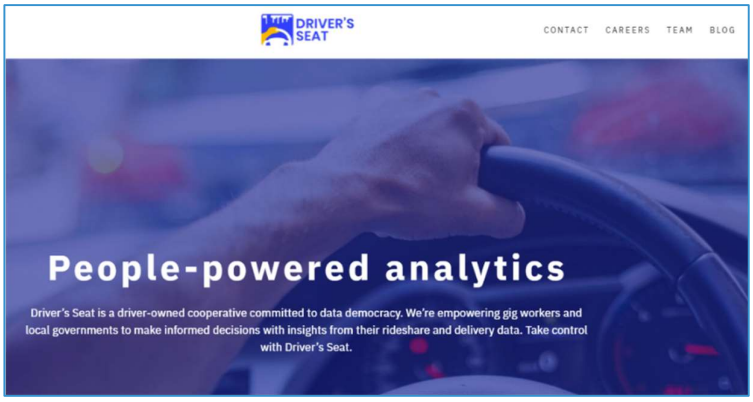


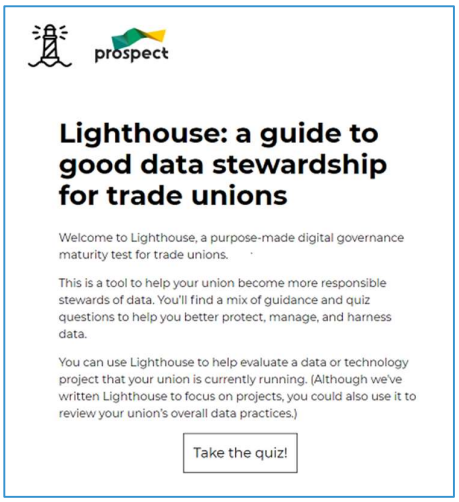
Figure 6: WeClock - an opensource tool for workers and unions. www.weclock.it

It can log app usage to help you prove when you are using work apps – a helpful tool against the "always on" work culture. It can log your location and movement to show how far you commute or travel for work, where you are, whether you are on your feet or sitting down. Do you get breaks? Are you compensated for the time spent? By logging when you enter work, it can support your campaigns on working time. With good data analysis and a group of workers' data, unions can begin the important journey of data storytelling pushing back on the employer-led or tech world work narrative that dominates much of our labour markets. WeClock can be used off-line and therefore also in geographies with high data costs. A union guide for how to use WeClock in organising and campaigning is available too.

Driver's Seat



Other inspiration can be found in worker data collectives. A really promising example of this is **Driver's Seat** – a cooperative in the US where on-demand drivers use the Driver's Seat app to track and share their data. What Driver's Seat can inspire us with is the collectivisation of data and the analytics of it to empower workers.



Lighthouse

A third helpful tool is an open-source guide to good data governance for unions. One thing is if unions start structuring the data they already have or get through new responsible tech, another is how this data is used and cared for to protect members' integrity and privacy. **Lighthouse: a guide to good data stewardship for trade unions** offered to all unions by the UK union Prospect helps unions do just that.

One thing is for sure: Industry-tech seldom comes with your members' or your union's privacy at heart. WhatsApp is owned by Facebook, who openly has filed for the cross-sharing of data between the two platforms. Signal on the other hand does exactly what WhatsApp does in terms of services for the users yet is fully encrypted and does not share or sell the data. Whilst WhatsApp is widely used, it could be a good strategy to meet members there, and gradually guide them over to using Signal.

Many unions store all their documents, spreadsheets, databases and emails in the Cloud, and thus are falling prey to the data extraction of mainly Microsoft and Google. New advancements in the so-called decentralised web where locally held servers interconnect in a privacy-preserving way, should seriously be considered by unions going forward.

Data Visualisation and Storytelling

Data from your members can tell a thousand tales. Data if rendered correctly is indisputable. It gives you proof. Visualising these data in graphs or images can really support your campaigning. It can boost awareness, sway public opinion, provide evidence to employers and help form an understanding of the reality of work from the workers' perspective.

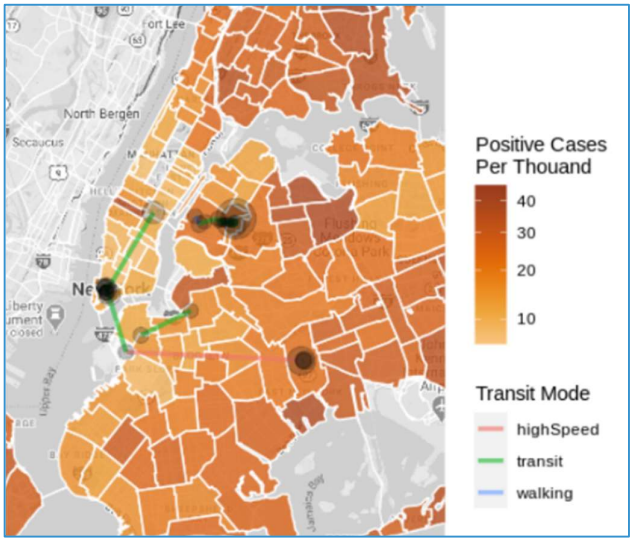


Figure 7: Data visualisation of location overlayed with Covid risk zone data. By Dan Calacci, MIT

Here are two examples.

WeClock was tested by union organisers in New York City. Let's imagine they were homecare workers. The image shows the workers' travel routes and whether they were walking or in transit. Publicly available data on the number of Covid cases in each neighbourhood in NYC was then overlayed the worker's movement data. What we see is that the workers had to be in, or travel through, high-risk zones throughout the day. This visualisation helps prove workers' risk environment. The location data is non-disputable. Using this can help support the union's demand for higher wages for homecare workers.

In another example, all workers in a workplace had WeClock installed and running. We used their location data to map throughout the day how often they were within 2 metres (6 feet) of one another. This to prove that the workplace's claim that social distancing measures were in place were wrong. The data visualisation can be seen in Figure 8.

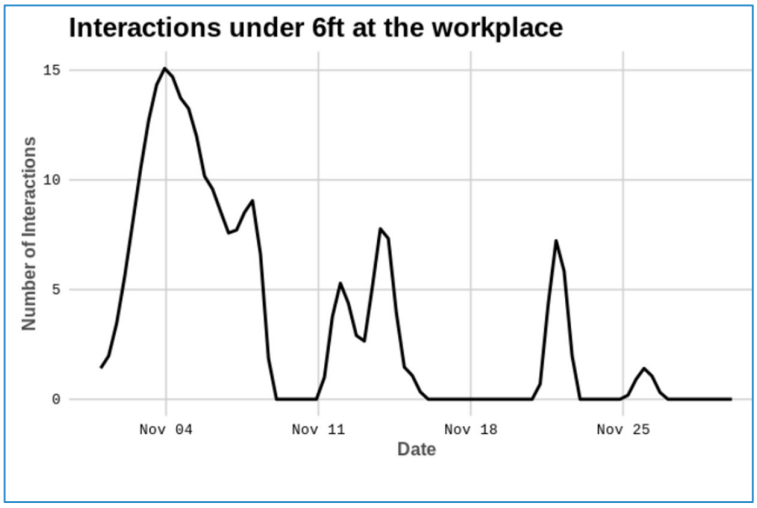


Figure 8; Worker interactions under 6 feet (2 m) over a time period. By Dan Calacci, MIT

Analysing and visualising data requires access to specialists who are trained to do just that. Whilst some really good tools exist such as R-studio and Google's Data Studio, using them effectively requires some practice and learning. Once you have, or have access to, these skills most of the impact comes through imagining what story to tell and what other data sources will support that story. Data Storytelling and Data Visualisation is like laying a multi-dimensional puzzle.

The circle diagram below sums up the journey unions should take to responsibly tap into the potentials of digital technologies:

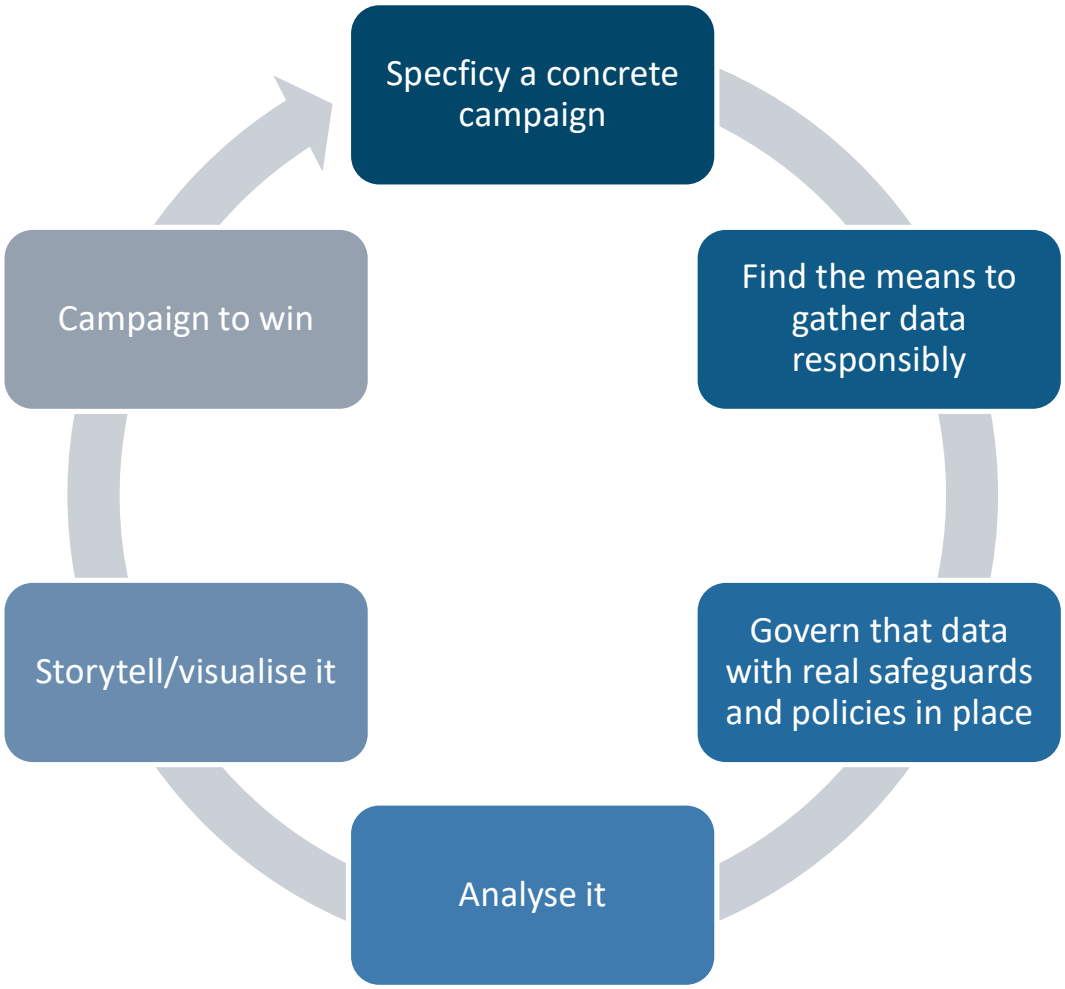


Figure 9: Process of digital campaigning

Summary of chapter

In this chapter we have looked at policies, collective bargaining themes and technologies and strategies that can be used to ensure decent work in public services. We have seen how current data protection regulations can be used to improve

workers' data protection and discussed where additional bargaining and/or policies are required to improve workers' data rights.

From there, we turned out attention to algorithmic systems in public workplaces. Acknowledging the potential discrimination and commercialisation in these systems as discussed in chapter 2, we set a number of requirements to public services deploying these systems. They should at all times be transparent around which systems are used and why. They should be able to answer our "who" questions, and a number of other questions that relate to ensuing public services have control over the systems deployed, who owns the systems, what contractual arrangements have been made concerning data access and control and editing rights. Without data access and control, public services will gradually lose the means (the information) required to serve the public.

We also showed a model for co-governing algorithmic systems – especially relevant for those that are used in human resource management. The Canadian impact assessment model was shown as an example, but also for what is lacking: namely the workers' voice and the important periodic reassessment of these systems.

From there, we borrowed inspiration from Just Transition policies and presented why all the introduction of disruptive technologies must be met with employer obligations towards the workers' job and career paths.

We ended the chapter looking at various ways unions could deploy technology responsibly to boost the workers' voice and impact. Here we particularly cautioned that much off-the-shelf technology does not have workers' rights at heart and that unions should lead the way in the transformation to more secure technologies. Several tools built for or by unions were presented that can safely be used to campaign for workers. Lastly, the art of data storytelling and visualisation was presented. Noteworthy here is that responsibly gathered data can be combined with other data sets to powerfully show a different story about the modern conditions of work that otherwise would not be seen.

In chapter 2, we discussed that digital technologies are bias and discriminative disfavouring the already disadvantaged. The current unequal distribution of power we identified and the commodification of labour can, by applying some of the tools and ideas in this chapter, be rectified.

Dig Deeper – Resources

Articles and reports	Valerio de Stefano and Simon Taes (2021) : **Algorithmic management and collective bargaining**, ETUI brief by https://www.etui.org/sites/default/files/2021-05/Algorithmic%20management%20and%20collective%20bargaining-web-2021.pdf
	De Stefano V. (2019) '**Negotiating the algorithm': automation, artificial intelligence, and labor protection**, Comparative Labor Law & Policy Journal, 41 (1), 1-32. Available here: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_policy/documents/publication/wcms_634157.pdf
	Adams-Prassl J. (2019) **What if your boss was an algorithm?** Economic incentives, legal challenges, and the rise of artificial intelligence at work, Comparative Labor Law & Policy Journal, 41 (1), 123-146. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3661151
	IFOW (2021): **The Amazonian Era – How algorithmic systems are eroding good work**. https://uploads-ssl.webflow.com/5f57d40eb1c2ef22d8a8ca7e/609ccc18ac8a6a30de7c5aee_IFOW%20The%20Amazonian%20Era.pdf
	Colclough, C. (2020): **Workers' rights: negotiating and co-governing digital systems at work**. Social Europe https://www.socialeurope.eu/workers-rights-negotiating-and-co-governing-digital-systems-at-work
	Colclough, C. (2020): **Towards Workers' Data Collectives. Article for A Digital New Deal**, https://itforchange.net/digital-new-deal/2020/10/22/towards-workers-data-collectives/
	Wachter, Sandra and Mittelstadt, Brent, **A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI** (October 5, 2018). Columbia Business Law Review, 2019(2), Available at SSRN: https://ssrn.com/abstract=3248829.
	Wachter, Sandra and Mittelstadt, Brent and Russell, Chris, **Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI** (March 3, 2020). Available at SSRN: https://ssrn.com/abstract=3547922 or http://dx.doi.org/10.2139/ssrn.3547922

	Ajunwa, I., Crawford, K., & Schultz, J. (2017). **Limitless worker surveillance.** California Law Review, 105(3), 735–776. https://doi.org/10.15779/Z38BR8MF94
	D'Ignazio, C. & Klein, F. (2016). **Feminist Data Visualization**. Workshop on Visualization for the Digital Humanities (VIS4DH), Baltimore. IEEE. (https://dspace.ceid.org.tr/xmlui/handle/1/955)
	Kresge, L (2020): **Union Collective Bargaining Agreement Strategies in Response to Technology**. UC Berkeley. Available: https://laborcenter.berkeley.edu/union-collective-bargaining-agreement-strategies-in-response-to-technology/
	Kresge, L (2020): **Data and Algorithms in the Workplace: A Primer on New Technologies**. WORKING PAPER, TECHNOLOGY AND WORK PROGRAM UC Berkeley: Available https://laborcenter.berkeley.edu/wp-content/uploads/2020/12/Working-Paper-Data-and-Algorithms-in-the-Workplace-A-Primer-on-New-Technologies-FINAL.pdf
	Shander, B. (2016): **NGOs, It's Time to Up Your Visual & Data Communications Game**. Medium. https://medium.com/@billshander/ngos-its-time-to-up-your-visual-data-communications-game-eb5ba769a5e8
	Rowland, C. (2019). **Your Next Fitness Coach Is... Your Boss?** The Washington Post. Retrieved from https://mrtechnews.com/your-next-fitness-coach-is-your-boss/
	DGB (2020): **Artificial Intelligence (AI) for Good Work.** Available here: https://www.dgb.de/++co++b7f96674-9f2e-11ea-a8e8-52540088cada/Concept-Paper-Artificial-Intelligence-AI-for-Good-Work.pdf
	TUC (2021): **Dignity at work and the AI revolution**. https://www.tuc.org.uk/research-analysis/reports/dignity-work-and-ai-revolution
	Owens, K., Walker, A (2020): **Those designing healthcare algorithms must become actively anti-racist**. Nat Med 26, 1327–1328 https://doi.org/10.1038/s41591-020-1020-3
	Corrine, C (2018): **Governing artificial intelligence: ethical, legal and technical opportunities and challenges**. The Royal Society. Available here: https://doi.org/10.1098/rsta.2018.0080

	Nield, D. (2020). **All the sensors in your smartphone, and how they work**. Gizmodo. Retrieved from https://gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002
	AI Now Institute (2018): **Algorithmic Accountability Policy Toolkit** https://ainowinstitute.org/aap-toolkit.pdf
Books	Noble, S. U. (2018). **Algorithms of oppression: How search engines reinforce racism**. New York University Press.
	C D'Ignazio, LF Klein (2020): **Data feminism**. Mit Press
Videos	Ethics of AI in the Workplace - panel @ OECD https://video.wixstatic.com/video/aeaf23_7376e49027e741548067cc27da72f1fa/720p/mp4/file.mp4
	Meredith Whittaker, ex-googler and since co-founder of the AI Now Institute 15 min speech on what AI is https://youtu.be/Ujvhqrbh5HM
	Dr Jonnie Penn: What History Can Tell Us About the Future of Artificial Intelligence, Ted X https://youtu.be/oW_VO5dwfRo
Courses	Data Ethics, AI and Responsible Innovation (edX), Edinburgh University (Started May 2021, but they could well repeat) https://www.mooc-list.com/course/data-ethics-ai-and-responsible-innovation-edx
Newsletters	Harvard Berkman Klein – for internet and society https://cyber.harvard.edu/getinvolved
	Exponential View by Azeem Azhar: https://www.exponentialview.co/
	Data Justice Lab: https://mailchi.mp/0a066951e8f4/subscribetodatajusticelabnewsletter
	Mozilla https://www.mozilla.org/en-US/newsletter/

Annex 1 – Benchmarking the GDPR

The GDPR defines personal data and Pii as: *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

In this article, DataGuidance and Future of Privacy Forum include a helpful comparison between the definitions of personal data in the GDPR and the CPRA

Recital 26 GDPR states that:

> *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*

This means that anonymised data sets where identification is 'reasonably likely' must be regarded as personal data. All else not.

However, as many experts argue, today, much economic value is derived from data that is not personal on its face but can be rendered personal if sufficient effort is put in place. This is really important for us to take note of. Anonymous datasets are really not that anonymous despite what the employers will say. We must ask whether the distinction between personal and non-personal data is a political one more than a realistic one. We must ask how workplace data that is not covered by data protection laws, can be used to negatively impact workers.

The GDPR – useful articles for worker empowerment

Whilst the GDPR offers a number of useful rights for workers, it also has its weaknesses.

Firstly, the useful rights from the workers' perspective:

1. **Data Minimisation**

The GDPR is founded on seven guiding principles. These are described in GDPR Article 5. A key principle is that of data minimisation (art 5(c)):

> *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

What article 5 says is that data controllers (the employer) may only collect the necessary data, and only the necessary data, for the given purpose and only the given purpose, and stored for only the necessary amount of time.

However, all is not that simple. Do we actually know what data processing is taking place? Although companies are obliged to tell you, do they? You have a right to be informed about:

- The collection of data
- How the company plans to use the data
- The reason why they are collecting the data
- Can the purpose of collecting the data be achieved without collecting the data?
- How long will the data be stored to fulfil the purpose?
- Is the data periodically reviewed in relation to the above 5 points and deleted if required?

2. **Editing and Erasure Rights**

In accordance with article 16 in the GDPR, you also have a right to edit the personal data collected on you, and article 17, gives you additionally the right to have the data erased if the data is no longer necessary to fulfil the purpose to which they were collected.

Article 17 is key to preventing that data and data inferences live on forever. Ensuring compliance with this article is therefore really important for the union policies of the right to a long working life.

3. **Data Protection Impact Assessments**

The GDPR sets out the legal requirements for Data Protection Impact Assessments (DPIAs). Article 35 GPDR states that a DPIA will be required where the processing, is

likely to result in a high risk to the rights and freedoms of natural persons. Accordingly, the use of personal data to monitor employees' activities requires a DPIA as such monitoring involves (i) systemic monitoring and (ii) data concerning vulnerable data subjects, owing to the "power imbalance between" the employer and employee.

Importantly, and often overlooked, article 35.9 further states that "the controller shall seek the views of data subjects or their representatives on the intended processing." In workplaces this means that workers' representatives (which includes unions) should be consulted by employers before the introduction of new data processes, including surveillance technology.

The predecessor to the European Data Protection Board, the Article 29 Working Party, further issued the recommendation that DPIAs are periodically reviewed and that the stakeholders (for us the workers) should be consulted as part of this review.

The UK trade union Prospect has put together a very helpful guide on DPIAs. Herein they recommend shop stewards to ask the following questions during a DPIA.

> *• How is the data going to be used? • Why is the personal data being collected? • What are the sources of these data? • How have you identified risks arising from the use of individual personal data and the rights/ freedoms of the collective group of employees? • What are these risks and how can they be reduced? • If you have decided not to consult with union reps, can you disclose the reasons why? • What will be the review process? • How will data breaches be shared with the union?*

4. Data Subject Access Requests (DSAR)

Citizens and workers alike have the right to receive all of the personal data a company or an employer holds on them. This includes regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.

Recital 63 of the GDPR states:

> *"A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing."*

DSARs are an important tool for worker empowerment. But note the wording in recital 63 on "reasonable intervals". An employer can refuse to fulfil their obligation to comply to recital 63 if the request happens too often or disproportionately so.

5. Right of Representation

Article 80 of the GDPR called "Representation of Data Subjects" gives a worker the possibility to mandate their union to lodge complaints on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf, where provided for by Member State law.

Article 77 is here interesting. It is concerned with the "Right to lodge a complaint with a supervisory authority". This means that a union can lodge a complaint on behalf of a member and thus support him or her throughout the complaint process. Note as well here, that in the GDPR a complaint can be based on proven fact, but also suspicion. Also that the national supervisory authorities are obliged to investigate all received complaints.

6. Processing in the context of employment

Lastly, a key article in the GDPR is article 88. It basically says that member states can by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.

Annex 2 – Data Protection Asia Pacific

GDPR adequate legislations or GDPR-inspired legislations	
New Zealand	New Zealand, Legislation, Privacy Act 1993 (in English) has GDPR adequacy, but this could be lost after the implementation of the new Privacy Act 2020 which is not modelled on GDPR. The Privacy Act covers information about an identifiable individual, and does not cover non-personal information. The legal basis for collection and processing of data is necessity for purpose. If an agency collects personal information, it is required to take steps which are reasonable in the circumstances to ensure that the individual concerned is aware that the information is being collected, the purpose for which it is being collected, and the intended recipients. The law provides for optional/voluntary privacy impact assessments. There is no mention of protection against automated decision-making. http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html
Japan	The collection, storage and processing of personal information is regulated by the Act of Protection of Personal Information. The law applies to private business operators, but not to public entities, entities, such as central government organisations, local governments, and incorporated administrative agencies. As mentioned, earlier, the legal base for consent is notification. Business operators can share personal information with a third party (parent and affiliated companies are considered third parties) within Japan only with the prior consent of the individual. Data subjects have a right to accuracy of data, security of data, record keeping and confirmation when third parties are involved, access and correction, disclosure and deletion. It does not provide the right to be forgotten, right to withdraw consent, or a right to data breach notification. No mention of protection against automated decision making either, no mention of DPIA. Japan has GDPR adequacy. Act on the Protection of Personal Information (in English, unofficial translation), http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
Thailand	Entry into force of the main operative provisions of the Personal Data Protection Act 2019 were deferred from May 2020 to 1 June 2022. Personal data is defined as "information relating to a person which is identifiable, directly or indirectly, excluding the information of a dead person." Explicit (express, in writing or through an electronic system) consent is required for collection, disclosure or use of personal data. For some cases, legitimate interest can also be a basis (Data Protection Report 2020). A data subject can request access to personal data, as well as submit requests to delete, destroy or anonymize it. Disclosure or transfer of personal data to third parties is prohibited, except with consent (subject to limited, customary exceptions). No mention of DPIA found. No mention of the right not to be subjected to automated decision-making.

Sri Lanka	The Personal Data Protection Bill (final draft released in 2021), modelled on GDPR, aims to protect personal data and regulate its processing under the constitutional right to privacy. It defines personal data as identifiable data of persons alive or deceased, and only leaves out 'irreversibly' anonymized data. It provides for consent for 'specified' and 'explicit' purposes as the lawful grounds. DPIA is to be carried prior to (large) data processing that is likely to result in a risk to the rights of data subjects. The DPIA has to be submitted to the government representative in charge, and therefore probably available for review.
Other comprehensive legislation	
Australia	Australia has strong data privacy obligations under the Privacy Act 1988. The legal basis for collection of personal information is reasonable necessity with notification, except for sensitive information which requires consent. Consent is also required for disclosure of sensitive information for direct marketing or use of data for a secondary purpose. Consent can be express or implied. Consent must be: informed; voluntary; current, specific; and given by an individual who has to the capacity to understand, and the ability to communicate their consent. Opt-out consent can be valid if properly informed. Consent can also be withdrawn. If consent is given, there are no substantial right to restrict processing of data. Australia regulates data protection through both federal and state laws. Privacy Act 1988, http://www.comlaw.gov.au/Details/C2015C00089
South Korea	The data protection laws consist of a general law, Personal Information Protection Act 2020, and several special laws pertaining to certain specific industry sectors. It provides very prescriptive and specific requirements for handling personal data. Due to the requirements of prior notification and opt-in consent, and relatively heavy sanctions prescribed by law, it is one of the strictest data protection regimes in the region. It covers personal data, Pii and anonymised data. Express consent is the legal basis for collection and use of personal data, exceptions exist and have been expanded in the 2020 amendments to the Act. NO mention of DPIA or protection against automated decision-making.
India	The Information Technology Act, 2000 covers data protection and violation of personal privacy. The storage, management and handling of sensitive personal data or information belonging to persons located in India is regulated by the Sensitive Information Rules enacted under the ITA. The government has released the Personal Data Protection Bill, 2019, which is being considered to replace the Sensitive Information Rules. The PDP Bill covers data that can identify an individual, directly or indirectly, as well as non-personalised data. It makes notice and consent the legal basis for processing personal data and for s specific purpose, while providing conditions under which data can be processed without consent. Consent can be withdrawn. The Indian government has wide powers to exempt any of its agencies from any or all data protection obligations under the PDP Bill for several reasons. Personal Data Protection Bill, 2019: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

	Information Technology Act 2000: http://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf
Singapore	the Personal Data Protection Act 2012 (PDP) deal with data collection, processing, or disclosure within Singapore. The Act does not apply to public agencies (including the government, ministries, departments or organs of the State, tribunals and statutory bodies); individuals acting in personal or domestic capacity; employees in the course of their employment; or business contact information. The legal basis is express and deemed consent, and is given after an individual is notified about the original/ revised purpose of collection of their personal data and voluntarily provides this data or when it is reasonable that the individual would voluntarily provide such data. Consent can also be withdrawn Data under the public agencies are bound by the Public Sector (Governance) Act, 2018. Data protections standards under the PDP and PSG Act are broadly aligned.
Malaysia	The Personal Data Protection Act 2010 (PDPA) through the PDP Department excludes the government sector from its scope. The PDPA requires that individuals be notified of data collection, give consent, and be informed about the purposes for which the data is being collected. The PDPA prohibits any disclosure of the personal information which is not pre-declared to the customer, and the information must be kept secure and not retained for longer than is defined in the privacy policy. Individuals must also be allowed to access their information that is stored.
Philippines	The Data Privacy Act (DPA) was passed into law in 2012. This made the country the second in Southeast Asia to promulgate a comprehensive data protection law. It was actively implemented only in 2016 with the establishment of the National Privacy Commission and the subsequent issuance of the statute's Implementing Rules and Regulations.
Partial legislation, or policy and regulations	
Brunei Darussalam	*The country is guided by a Data Protection Policy which covers personal data (in electronic or manual form) managed by government and educational institutions.*
Indonesia	Law No. 11 of 2008 on Electronic Information and Transactions restricts the electronic use of private data. Consent is the basis for processing personal data, explicit consent is required for the collection of sensitive personal data. Operators can process data only for the stated and approved purpose for which it was collected. Sharing of data with third parties requires the consent of the individual. There is no mention of protection against auto moated decision making, or of DPIA. A new draft of the Data Privacy Law has been prepared but has not been introduced yet (as of 23 April 2021). It is reported to be a GDPR-style comprehensive data protection law, that will replace the existing legislations and apply to the government and the private sector.
Laos	*Has enacted laws with cover provisions relating to the protection of personal information—Law Protection of Electronic Data (2017) and Law on Prevention and Combating Cyber Crime (2015).*

Myanmar	The country's Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017) law prohibits interception of citizen's electronic communications, private correspondences and physical privacy, unless otherwise warranted by an "order".
Vietnam	Has laws regarding Cyber Information Security (2016), Information Technology (2006), E-Transactions (2005), and a law on Protection of Consumers' Rights (2010). Article 21 requires that individual's consent is a must for the subject's data to be collected, processed, or used, and mention the purpose for which it is being collected. The individual can request to personally manage the information and the information controller or processor must immediately take the necessary measures.
ASEAN	The ASEAN Framework on Personal Data Protection states the principles on data protection to help the members in the implementation of domestic laws and regulations aligned with the global framework.
Nepal	The Privacy Act, 2018, legislates on the usage of personal information. It provides a limited definition of personal data that does not include Pii. However, it provides that personal data may only be used 'for the purpose for which it has been collected', or with consent, and some personal data cannot be disclosed without consent (Law Commission Nepal). In addition, the controversial Information Technology Bill, 2075 (2018) covers information technology, cyber security, and data protection. It prohibits the collection of personal information of individuals, unless it is otherwise permitted by law, and sets the conditions for collection and storage.
Pakistan	Pakistan has an e-commerce policy (2019) and a Personal Data Protection Bill, 2018 (aligned with the second-generation EU laws, rather than GDPR) which only covers commercial translations (the private sector). It provides for lawful grounds for processing personal data, requirements for minimal processing, rights to withdraw consent for processing data, and a right to erasure.
Bhutan	The Information, Communications and Media Act of 2018 covers personal data and includes seven of the ten 'second generation' principles found in the 1995 EU Data Protection Directive, making it a moderately strong law.
Tonga	Privacy and Data Protection: Legislation

No legislation

	Cambodia, Samoa, Fiji, Bangladesh, Maldives **Note:** The issue of data protection has been dealt with in a very limited manner under Section 18 of the Bangladesh Digital Security Act, which provides that if any person "collects any data or data storage"; then the said person person's activity will be a punishable offence under the Act