ZeMKI COMMUNICATIVE FIGURATIONS

ZeMKI Working Paper | No. 41
ISSN 2367-2277

Phoebe V Moore

Problems in protections for working data subjects: Becoming strangers to ourselves

Universität Bremen ZeMKI Zentrum für Medien-, Kommunikations- und Informationsforschung

Universität Bremen | University of Bremen
ZeMKI, Zentrum für Medien-, Kommunikations- und Informationsforschung
Linzer Str. 4, 28359 Bremen, Germany, E-mail: zemki@uni-bremen.de
www.uni-bremen.de/zemki/ | www.uni-bremen.de/en/zemki/

Phoebe V Moore (p.moore@essex.ac.uk)

Prof Dr Phoebe V Moore is Professor of Management and the Futures of Work, University of Essex School of Business and Senior Research Fellow, International Labour Organization Research Department. In 2021, she was ZeMKI Visiting Research Fellow at the University of Bremen. She has been writing about work and worker struggle since 1997 when she lived in South Korea during the East Asian economic crisis, and her research highlights specific pressures workers face in contemporary and historical context. Her current research looks at the impact of technology on work from a critical perspective, looking at quantification through wearable tracking and algorithmic decision-making as a set of management techniques where control and resistance emerge as well as new risks of psychosocial and physical violence (2015, 2016, 2017, 2018). Her previous work looked at the role of trade unions in international development and poverty policy in relation to International Labour Organization’s multilateral relationships (2014); subjectivity and the radical potentials of non-proprietary peer to peer production linking workers across virtual spaces (2009, 2011); and the globalization of worker education from a neo-Gramscian perspective where hegemony is not yet solidified, evidenced through consistent worker uprisings internationally (2005, 2006, 2007).

Working Paper No. 41, June 2022

Published by ZeMKI, Centre for Media, Communication and Information Research, Linzer Str. 4, 28359 Bremen, Germany. The ZeMKI is a Central Research Unit of the University of Bremen.

ISSN: 2367-2277

Problems in protections for working data subjects: Becoming strangers to ourselves

1 Introduction

As Thales of Miletus challenged, 'the most difficult thing in life is to know thyself'. What this ancient philosopher would never have imagined perhaps is now a question we can reformulate: 'the most difficult thing in life is when artificial intelligence knows thyself'. Over the past thousands of years, the concept of self and being have driven a great deal of Western philosophy. Now, we are now able to take quite seriously a new actor in the field of self-framing: that of machines. Given the increase in data usage by people and organisations for what is often access to basic services, and the seeming imminence of widespread application of AI into business operations globally, the idea that data can be used to create versions of selves, or what I will discuss here as 'data subjects', is itself quite new when framed against a history of philosophical questions.

Data has become a very valuable asset, and its capacity to define 'subjects' and to help management to define subjects is built into the epistemology of technological integration processes which begin to introduce AI and other products into workplaces.[1] An increasing number of human resources and other workplace/space decision-making systems have begun to include AI-systems, where semi-automation of cognitive tasks associated with worker selection and talent management is underway at worrying rates (IFOW, 2020: 6). The seeming final frontier within these spaces are systems that are called 'AI' which become seemingly agential with decision-making power that rivals or 'wins' against human competence. Natural persons, who are humans, are identifiable 'data subjects' as labelled within data privacy law e.g., the General Data Protection Regulation (GDPR). Technically, we have more rights to access and control data about ourselves than ever before, based on this now-live European Union wide Regulation. Updating the Data Protection Directive 95/46/EC and the 1998 Data Protection Act, the GDPR:

> […] significantly changes data protection law in Europe, strengthening the *rights of individuals and increasing the obligations* on organisations. (Irish Data Protection Commission, 2019, italics added by current author)

Increasing the rights and protections of individuals and putting more obligation onto organisations sounds wonderful and the idea that there can be better data and privacy protections for workers is altogether progressive. However, the use of the term 'subject' in policy implies several things. Firstly, that *subject* is somehow a homogeneous category that can be represented as such; secondly, and perhaps more philosophically than policy can really acknowledge, that a subject can be known, at all. Thirdly, data policy largely omits the recognition of a key point about humanity, that we operate based on social relations. Indeed, data collection is a social relation.

[1] These days, the concept of the place for work is contestable not least in the current working from home movement driven by Covid-19 and its antecedents, where the increased expectation for exogenously provided environments has diminished at least in knowledge and office work. Perhaps 'workspace' is a better term, given this, which I have argued elsewhere (Moore, 2020a). Daniel Dennett, in the 1990s referred to 'workspace' philosophically which future research could consider, where he speaks of a workspace as a plane for consciousness where past, present and future form the working memory (1992: 139–170 as cited in Hayles, 2017: 42).

Perhaps the best-known theorist of the 'subject' is Michel Foucault, who wrote that 'there are two meanings to the word "subject": subject to someone else by control and dependence; and tied to his own identity by a conscience of self-knowledge' (1982: 782). *To be subject to* involves a power relationship; inequality; degradation; violence. Subjection entails the submission of subjectivity i.e., where a subjectivity is determined by a process which is not individually decided or chosen, whereby:

> […] all types of subjection are derived phenomena, that they are merely consequences of other economic and social processes: forces of production, of class struggle, and ideological structures which determine subjectivity. (Foucault, 1982: 782)

However, the 'conscience of self-knowledge' Foucault (1982) talks about as a form of self, is where possibilities for self-freeing subjectivation emerges. Butler is clear that subject formation means finding autonomy of the self, and 'giving an account of oneself' is one of the most important nodes in a process of subjectivation or freedom of the self and selves (Kim, 2011). Where this is absented, vulnerabilities are exacerbated. Today, what is now known as 'algorithmic management' (Rani & Furrer, 2021; Rosenblat & Stark, 2016; Woodcock, 2021) takes on what Evans and Kitchin speak about as a 'modulation' approach, involving subject prescriptions and 'subjectification'[2] made with insufficient accountability, which may eviscerate or at least put an obstacle in the way of emancipatory 'subjectivation'[3] (Evans & Kitchin, 2018) for the worker subject category – who is, despite these new levels of abstraction, are by no means liberated within working relationships today.

The increase in the uptake of algorithmic management and platform digitalisation at work as leading to ultimately the empowerment of an ideal type, the supposed 'algorithmic boss' (Adams-Prassl, 2019), where numeration is expected to at least complement management and improve decision-making and leadership. Given what I am arguing here, we should revisit what is at stake for adequate protections for data subject *workers*, when our data is used by external entities to profile us, in ways that are often completely outside of our control and where profiling is commonplace for advertising agencies, public bodies, banks *and* our employers and clients. As data is increasingly hoovered up by the powerful market dominators in so many areas of life, this question is becoming increasingly difficult to ask, much less to answer. Bloom writes that the *owners of data own the future*, but he reminds us that this is not an ideologically neutral historical point and currently we are embedded in a capitalist model for social relations (2019: 2). While technology's predictive capacities may technically surpass humans', because of the political economy within which social relations exist, prections are not automatically objective - nor are they necessarily correct.

Building on these arguments, I want to look at the problems in constructing and relying on social protections for workers, by querying the depiction of the data subject in the policies that should protect workers, highlighting the scarcity of engagement with conceptualisations of the complexity of the subject, and the failure that presenting a subject as though it could be positioned homogeneously at all, reflects. With that in mind, this piece intends to unravel a series of considerations for the data subject to demonstrate why current data protection policy does not sufficiently protect all subjects identically by way of the failure to sufficiently delineate subject types and because of the failure to recognise that all social relations are not equal. Then, I assess theorisation of the subject from a cross-disciplinary perspective, arguing that the contemporary uptake in worker profiling differs from previous forms where a 'boss' could be known. While the GDPR is written with

[2] Subjectification is a Deleuzian concept, where subjects are prescribed characteristics exogenously (see Deleuze, 1995).
[3] Subjectivation is primarily a Foucauldian concept, involving the discovery of agency and empowerment against an aggressor.

a human focus, the AI Act draft now under consideration removes this category and focusses on providers (companies producing AI products) and users (companies buying and applying AI products). AI systems at work do more than collect workers' data, however. They may require workers to work directly with machines or against machines, depending on the company. They may work entirely independently in a semi-automation scenario where chatbots do some of the work and replaces tasks that a worker once did.

A worker is a complex identity. Workers derive significant meaning from their work, after all, and risk losing their (our) sense of identity and subjectivity, as work is stolen from them (us), by AI. Worryingly, though the AI Act puts increased obligations on providers and users, the recognition of the precise actor who will be most impacted by technological integration into work is largely overlooked, and thus social relations and human machine interaction dimensions are assumed to have protection on the basis of a range of risk judgements or based on other regulations that are intended to cover specifics such as risks for workers that AI systems may introduce. While AI is classified with levels of risk in the AI Act, there is no conceptualisation of specifically *how* humans face risk because of the systems, nor how specific decision-making AI systems *in fact, themselves,* depict risky subjects.

Overall, in this piece, I ask, what happens to/with worker subjectivities and worker agency when data is used to formulate and portray specific profiles and portrayals of ourselves, a process Althusser talked about as 'interpellation'?[4] Who do we 'become' when the choices to derive our 'selves' diminish? The pursuit of datafication (Van Dijck, 2014; Kennedy, Powell & Van Dijk, 2015) and data-based profiling of the human subject only occurs between humans in everyday circumstances (Couldry & Powell, 2014) and perhaps that is a key feature which sets us apart from other species. Importantly, who will have the right to what Deleuze and Guattari talk about as 'enunciation' (Deluze, 2014; Guttari, 1987), or the right to formulate a subjectivity and agential self? Will data regulation provide adequate worker protections which can enable not just basic rights but even agency formation and subjectivation?

2 GDPR and the AI Act: The data subject in policy

A person whose data is being gathered and used to make decisions and create profiles about them, is instantly the subject of a social relation, and subject decisions and inferences made based on the data collected about them. Because the data subject concept is expected to refer to all identity capacities for all (European) humans in all roles and characteristics that natural persons embody and adopt, the debates about the emancipatory potentials of data sharing and ownership made possible by new Regulations must be counterweighted with new formulations for questions of privacy and data protection of *datified* selves, where recursively, the precise act of collecting and using data about natural

[4] Althusser describes a 'theoretical theatre' (1970) wherein a theorised person such as a policeman, calls out to another person on the street: 'hey, you there!', at which point the said person who is hailed, is considered a possible suspect immediately, whether or not they have done anything wrong. This process becomes an interpellation of individuals as subjects, whereby someone's subjectivity is narrowed down to a specific identification, which Althusser talks about as features of ideological processes rather than as accidental. Using data to make decisions about individuals has similar implications if occurring within the workplace, because of the power relations between e.g., a manager and a worker. This can be compared to the notion of a police officer and a civilian. A police officer has state-sanctioned violence in her/his job description. A manager holds power over a worker's basic access to sustenance and livelihood. Collecting and using data about a worker holds distinct possibilities for interpellation.

persons profiles us into specific categories which may or may not cohere with an individual's understanding of their perception of a self. This is probably because a) the 'self' is not an inherent category, b) each human self is constituted of many selves within one body, sometimes even simultaneously (e.g., see 'prosumer', Fuchs, 2011 and following sections), and c) overall, the questions of becoming, agency, or other notions of emancipation of the self, cannot be fully dealt with, when using this limiting, but far from neutral, policy category.

The data subject was originally termed as such within the 1995 Data Protection Directive, then the Data Protection Act 1998 and now, the GDPR. These Directives, Act and Regulation have been formulated to deal with how new technologies on the market designed to collect new data in all sorts of ways should be implemented; and formulated requirements around this as applied to all 'data subjects'. The data subject can be a consumer, a citizen, a criminal, a black person, a gay person, a religious person, a worker, and so on. There is no separate definition of the data subject made available even within the Definitions section of the GDPR, but in Art. 4, the definition of 'personal data' helps, where the term 'data subject' appears within parentheses after the phrase 'natural person':

> 'Personal data' means 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. (GDPR, 2020, Art.4)

The Cornell Legal Information Institute's definitions for a 'natural person' is:

> A living human being. Legal systems can attach rights and duties to natural persons without their express consent. (Cornell, 2022a)

This can be contrasted with an 'artificial person', who is:

> An entity established by law and given at least some legal rights and duties of a human being. Corporations are the most common types of artificial persons. (Cornell, 2022b)

An overview of related policy and existing academic literature and surrounding debates shows that much of the delineation between different classifications of 'subjects' are mostly inferred rather than made explicit, outside of the areas of defined protected characteristics. The conjoining feature of data subjects is simply that we are natural persons, or 'living human beings' and that rights and duties can be ascribed 'without their express consent'. This is significant for two reasons. Firstly, human/computer interaction and AI research would not have begun, nor would it currently exist, if we did not possess the capacity to define ourselves as 'living human beings' and therefore to differentiate ourselves e.g., from machines and corporations. There has been extensive discussions regarding whether machines should be attributed with electronic personalities or legal personhood (see Avila Negri, 2021 and Special Issue edited by Gunkel et al, 2022). In 2017, the European Parliament made recommendations ot the Commission on Civil Law Rules on Robotics to consider giving sophisticated autonomous machines such a label (electronic personality). The proposal was responded to with an Open Letter in 2018, signed by over 150 experts in the area, who strongly refute the idea that robots should be granted legal personhood. Then, the AI Act draft does not mention this at all. So, it does not appear that machines will be attributed with personhood any time soon. Secondly, the concept of *consent* is used to distinguish part of the relationship between a legal system and a living human being, whereby the latter's attributed rights and responsibilities can be given without a subject's consent. The absence of consent has quite different connotations depending on

which subject category is in the frame for consideration as I discuss below. Indeed, data subjects have far more relationships with far more other subjects than with the data protection officer (DPO) alone (Abraha, 2022), lending far more complexity to any notion or likelihood of consent.

The *Data Protection Directive* 95/46/EC provided the first binding international instrument designed to protect people's privacy where organisations collect and process personal data; and to regulate personal data flows across borders. Its advancement of privacy law owes a lot to the OECD's *Privacy Principles*, which are part of the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The OECD's projects apply more globally than European policies and these Guidelines were developed in the 1970s and were fully introduced in the 1980s. The OECD *Privacy Principles* were incorporated into the 1985 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, which are closely linked to the European Commission Data Protection Directive 95/46/EC (Custers & Ursic, 2018: 330). The Guidelines do not contain a specific definition of the data subject, but Part One, General Definitions indicates

> For the purposes of these Guidelines: […] b) "personal data" means any information relating to an identified or identifiable individual (data subject). (OECD, 1980)

So here, the data subject is an 'identifiable individual', rather than what followed in the GDPR, which calls the data subject a natural person as discussed above, which in essence collapses identification with subjectivity.

A 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016' was introduced to deal with the protection of data subjects regarding processing of personal data, and on the free movement of such data. This was becoming increasingly relevant partly because of the immense amount of data being shared on social media platforms and other lucrative arenas as well as the acceleration of global labour markets. Emerging case law such as Bărbulescu v. Romania, a case that started in 2007 where personal communications data was used to terminate the employment of a sales worker, who had used a work messenger service for private conversations. That, and because of other legal cases around that time, made it clear that data and privacy protection law was not fit for purpose. The above-mentioned Regulation had been introduced to protect natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, which had been linked to the repeal of Council Framework Decision 2008/977/JHA (Eur-Lex, 2019) and the repeal of Directive 95/46/EC, but while these initiatives helped to allow data sharing to identify criminal behaviour, these repeals and updates were evidently not enough to positively protect workers and other citizens. In that context, the introduction of the GDPR came about.

In 2016, the EU adopted the GDPR. Member States were given two years (2016 - 2018) to work to ensure that it is fully implementable into local regulation and in 2018 as of May, the GDPR was recognised as law across the EU. With horizontal effect, states were/are required to integrate the Regulation into local policy. As such, national legislation in the European Economic Area (EEA) must ensure adherence to the GDPR and all other actors in countries hoping to do business with European companies are also liable. The protections that can be applied for workers emerging from the GDPR are significant, nonetheless, and improve the Data Protection Directive 95/46/EC significantly. An improvement on the Directive is the emphasis placed on the importance of *data minimisation*, where a Data Controller (usually the company or other organisation collecting data) should only gather data that is specifically necessary to carry out the intended goal – which must sit within the criteria for lawfulness, can be used to negotiate over the purposes for the use of

technologies for workplace monitoring. Further to this, the data collector must demonstrate *proportionality* when setting out to gather data, meaning a company should demonstrate the balance between the needs and intentions of the organisation, and the rights of workers.

Art. 6 of the GDPR sets out the criteria for ‘Lawfulness of Processing’, indicating that data collection, processing and use is lawful ‘only if and to the extent that at least one of the following applies’ (GDPR Art. 6 2020):

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. processing is necessary for compliance with a legal obligation to which the Controller is subject;

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;

6. processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In other words, a Data Controller must carefully consider whether at least one of these criteria can be defended as a legal reason for data collection and use. One or more criteria must be defensible and should be communicated to data subjects clearly in all cases where data processing is carried out. Clearly, any consideration of worker/employer transparency is complicated by the variable dynamics, organisational history, and other aspects of specific work environments, but there are clear possibilities for advancement for data subjects’ rights, nonetheless.

While the GDPR significantly advances previous law, where, fortunately the identification of a ‘natural person’ and their experiences is made explicit (far more than within the AI Act, as we will see), much of the ‘what is at stake’ question is left to the readers’ interpretation in data law as to *who exactly* the natural person is, in each case. Purtova argues that there are many problems still with ‘identification’ in data law such as the GDPR, where data collection is used to create ‘identifiability’, but so far, there is not much to discussion or recognition of what happens once the natural person is ‘identified’ (Purtova, 2021). Of course, policy must be written in a way that allows a malleable subject category that can apply to as many cases as possible. However, phenomenologically and in our everyday and everynight lives, what makes us human at all, is in fact, that we experience social relations, and that we can ‘be’ more than one subject at once.

GDPR: Consent

'Consent' is the *first* identified criteria for defence of lawfulness of data collection, but it is hard to imagine authentic consent in an employment relationship. Consent is defined as follows:

> When a person voluntarily and wilfully agrees to undertake an action that another person suggests. The consenting person must possess sufficient mental capacity. (Cornell, 2022c)

Even within these definitions it becomes clear that at a fundamental level, it is tricky to say that all subjects are identical nor that all data subjects' relationships with other data subjects are identical. Indeed, 'choice' to use a product, based on data provided by consumers; and 'consent' for data collection in an employment relationship; are not identical transactions nor dialogic experiences containing identical capacity for 'voluntary' and 'wilful' actions on both sides. The synthesis of specific actions cannot be held in equal measure depending on subjects. This matters, because e.g., the first criteria for lawfulness within the GDPR is indeed, 'consent' and while there are loopholes and data controllers are able to select other criteria of lawfulness for data collection, A consumer's capacity to consent may be easily blurred with the idea of 'choice', and their possession or agency in that social relation with a company, and a workers' capacity for choice to do work or not[5]; are epistemologically antagonistic. Trzaskowski argues that there are imbalances of power in 'business-to-consumer' relationships too, but even so, workers are less likely to have freedom to choose to consent or not (2021: 68). This legal scholar argues that consent is 'not problematic' when:

a. the consent is properly informed

b. the user can withdraw consent to the processing of personal data

c. the user is properly informed about the right to withdraw consent. (Trzaskowski, 2021: 69)

Consent, however, requires a *line of communication* to actually exist first and for a data subject to have consciously made a decision which is genuine and informed. In all interviews with workers for my European Parliament report (Moore, 2020a), no worker was given information about what data would be collected about them, why the data would be collected nor how it would be used. While the sample was relatively small, it reflects the endemic lack of dialogue between workers and bosses around use of data. Perhaps what is necessary is to explore the provocation Antonio Gramsci set before us at the beginning of the last century, with his thesis on 'coercion plus consent', whereby people are unaware of their own exploitation but have made some gesture of consent all the same (Gramsci, 1971).

The epistemological set of supposed choices between affective joy or sadness whether at work or in the supermarket, are not, ultimately, endogenous categories. Lordon notes that the worker/employer consent relationship can never embrace a co-linearisation of relationships which would be expected for workers to embrace the full dream or promise of e.g., the product they are selling. Subjection, 'even when it is happy, consists fundamentally in locking employees in a restricted domain of enjoyment' (Lordon, 2014: 107). Worker data subjects only exist within a relationship of dependence due to material needs and in a social form where reproductive labour is performed by necessity and without recognition. Frédéric Lordon writes about consent in the working environment discussing Spinoza's and Baranski's theses on the sovereign subject and affect. Consent relies on an 'exogenous requisite' for producing what appears to be 'endogenous motivation, where

[5] Note Herman Melville's parable where the worker the Bartleby the Scrivener, states 'I would prefer not to'.

management leads data subjects into a position where 'they think that they are not led… but living after their own mind, and according to their free decision, where the 'institutions of capture' are enlisted. Joyful affects may be operationalised, a seeming love for a workplace, and so on (Lordon, 2014: 98). However, consent is a relation that is set against a background of violence, a 'backdrop of threat' where seemingly passionate servitude depletes agency within what Hayles (2017) speaks of as the unconscious. In these ways, it is difficult to understand how a data subject can be expected to provide consent, at all.

GDPR: Role of DPO

The GDPR requires a DPO to be appointed, for any organisation with over 25 employees. This is an important position. The DPO should actively seek consent from workers for data collection, processing, and use and consent should be considered at both the individual and the collective level so, both via individual lines of communication and through discussions with trade union and/or worker council representatives for a collective response likewise. DPOs should consistently reach out to workers to check whether their consent is still up to date; should give workers the chance to withdraw consent; should always report data breaches and violations immediately and ensure to correct these; should carry out data protection impact assessments (DPIAs) (Pakes, 2020); and should organise and advertise training in data collection alongside the obvious bureaucratic obligations for compliance.

AI Act

Partly as a response to a rising concern for increasingly widespread use of AI systems, in a variety of organisational and societal contexts, including the workplace (which requires data collection), the current European Commission's AI Act[6] draft is in circulation (in first quarter 2022). The draft Act outlines the prevailing 'AI Techniques and Approaches' of organisations as follows:

> a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
>
> b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
>
> c) Statistical approaches, Bayesian estimation, search and optimization methods. (EC, 2021, Annex 1)

This definition is not intended to define AI itself more metaphysically (Lilkov, 2021: 168), but rather attempts to list technical details of the AI systems being implemented. There has been significant debate surrounding the definition, because too much description may be interpreted to mean all software not listed would then be permissible, but even an all-encompassing definition does not capture the nuance that exists within device and software usage and both the technology's possible uses and human interpretation. Discussions leading up to the AI Act were hoped to be rigorous, where the high-level expert group on

[6] The longer title of this Act is the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts {SEC(2021) 167 final } – {SWD(2021) 84 final} – {SWD(2021) 85 final} (Brussels, 21.4.2021).

AI had presented the *Ethics Guidelines for Trustworthy AI* to the EU in 2019. The GDPR, puts increased responsibility on companies and organisations for responsible behaviour in data collection.

The AI Act requires technology providers to inform users[7] about how the provided product, e.g. the technology, works, so that companies can create good codes of conduct for usage. Potentially problematically, 'users' are defined as the companies who are buying such products and writing such codes of conduct, and the 'data subject' concept does not appear. In that way, the AI Act is digital single-market focussed, rather than human-focussed. However, it does aim to advance earlier legislation with the identification of *levels of risk* in the implementation of AI. In this way, the classification rules for defining a series of category of risk-identification in AI-systems, are oriented around whether these systems should be banned on the one hand, or regulated, on the other. The practices of interest for the current article's argument are 'high-risk AI systems', because they are not altogether banned, in the way that technology imposing 'unacceptable risks' in Title II, are. So, AI-systems are considered to be 'high risk' in the following areas:

- biometric identification and categorisation of natural persons;
- management and operation of a critical infrastructure such as road traffic and utilities;
- education and vocational training;
- employment and worker management [detailed below];
- access to and enjoyment of essential private and public services such as benefits and services;
- assessments of creditworthiness and emergency medical responses;
- law enforcement;
- migration and border control management; and
- the administration of justice democratic processes.

Criteria identifying 'high-risk' that is specific to the *employment* context is identified in Annex III:

> (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
>
> (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships. (EC, 2021, Annex III)

Many of the key decision-making processes experimented with so far in machine learning and algorithmic governance in platform work and human resources processes, such as people analytics, are in a high-risk area. Organisations wishing to integrate high-risk AI-systems into their data collection and surveillance frameworks will be required to ensure they follow a series of guidelines that provide transparency, robustness, accuracy and

[7] 'Users' are the companies purchasing technology packages with AI utility and application (NOT the workers or the consumers who are impacted by such technologies).

traceability of data and documentation (EC, 2021, 3.3. Impact Assessment, 9). Users, who are the organisations intending to implement high-risk AI systems, will be expected to follow instruction manuals for compliance that providers are required to include with such systems. Users should devise internal codes of conduct which commit to human oversight. Indeed, the definition of AI provided so far makes it very clear that humans define the objectives for AI to come to ‘life’:

> Artificial intelligence system (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of *human-defined* objectives [italics by present authors], generate outputs, such as content, predictions, recommendations, or decisions influencing the environments they interact with. (EC, 2021, Article 3, 1: 39)

Now, I begin to outline my thesis on how the move toward increased profiling and datafication of workers puts us in danger of becoming altogether strangers to ourselves, where our subjectivities are exogenously depicted and restricted via processes of numeration.

3 Working (risky) data subjects

Most people are not fully aware of how profitable their own data is, nor how necessary it is, for digitalised markets and workplaces/spaces to operate. It might not even be possible to be fully aware of the sheer amount of data being collected about you at any point in the day – e.g. how many times a CCTV camera catches your face; how much data Apple has captured from your ‘health’ app sitting in the background of all your movements; how many times you have looked at a website to decide whether or not to book a venue for an event; there may even be items of data you don’t realise have been inadvertently ‘collected’, such as your voice in the background of a recorded voice message someone else is recording in an open office context.

Even when people are somewhat literate on data, we, without knowing, not only surrender data to market and management hierarchy, but also surrender personal (political) agency, even subject to the ‘encoding of human agency’ (Introna, 2011), not just because it is nigh impossible to know about all data being gathered, making it very difficult to protest all of it; but also because there is very little incentive outside of the regulation discussed above, for companies to be transparent and to somehow share that information with you. This is perhaps because the more you know, then the more power to make decisions you have i.e., to opt out, to refuse, or to refuse to give, or to withdraw, consent, after it has been given. Given the invisibility surrounding accountability which so many algorithmic management processes retain, it is not even clear to whom or to what one is consenting. For these reasons, there is a significant consent deficit within the data accumulation regime. Indeed, the use of data to make decisions about workplace requirements for behaviour and practices can be shaped without full human, or at least, without workers’ input, at all.

Bringing together arguments from feminist, new materialist, and post-autonomist debates, and building some on key philosophers’ concepts, I want to encourage a debate that must be had about what is currently at stake for workers in the informated, smart workplace. The expectation is that the natural person must be nothing other than a docile whilst also productive body. The depiction of which subjectivities are considered acceptable in neoliberal contemporary lives is hardly obscured but is mysteriously meant to emerge by way of numeration and processes of profiling and datification. Using policy terminology of the data subject, I argue that we are facing a new digitalised era of workplace data subjectification, where other forces make decisions about which kinds of subjectivities are

permissible in the contemporary workplace: subjectivities that pose the least risk to employers and business.

Being a risky data subject

The worker data subject is in danger of being defined and labelled externally to autonomous selves via a range of forces, namely through human resource management channels which serve to create individualised profiles, where subjectivities are narrowly permitted for identification in ways that allow management to identify risky subjects. 'Worker' as a category itself, is not universally definable, given the variation in contract types (i.e., employee; self-employed; agency worker; zero-hours contracted; independent contractor including the bogus self-employed; etc.), however, work in capitalism is couched in a set of social relations that do not mirror those experienced when one is acting as a 'consumer' and 'citizen'. All types of data subjects are technologically monitored (Bloom, 2019); all subjects experience data theft as a 'technological form of alienation' (Andrew & Baker, 2021: 574), where data is endemically 'ripped from [our] lives' (Zuboff, 2019: 377). I want to argue that the relational and material experiences and the sheer possibility of a priori agency across categories of subjects, even workers who work with different kinds of contracts, is not identical. Agency to speak out against algorithmic decision-making likewise is not identical across categories either. Power relations between managers and employees and workers are, as indicated, very different from the relationship between a consumer and a corporation, or a citizen and the state. The depiction of the risky subject may not be known to the subject at all, such as in the case of CV rating systems, where someone's terminology on an application is not correct, or someone's loan is not approved. Sometimes a data subject is told they are risky, sometimes by notification such as in the case of taxi driver deactivation mentioned below.

Deleuze and Guattari discuss the dangers of delineation of subjects via what they call a 'linguistic machine', where the parameters for people achieving understanding of themselves are reliant on already defined grammars. This can result in a paradox of anxiety, given the supposed liberatory potentials the 'project' gives us (Boltanski & Ciapello, 2007) and the supposed self-fulfilment that companies that advocate for self-management at work seem to offer. A process of becoming a 'true' self was probably already unavailable within any workplace, given the already existing unequal power relations between workers and bosses. Instead, information accumulation results in newly enhanced surveillance regimes, where data is used to define and delineate subjects in ways that workers increasingly have no say in. There is a considerable binary in perception for contrast between machines on one side and humans on the other, otherwise we could not describe 'automation' as it is commonly understood to occur i.e., one job is replaced by one machine. Indeed, rather than consideration for what data collection does to the concept of the self, formation of the self, and right to the self, research on the human experience of data collection and our rights has mostly looked at consumer rights and more formulaic questions relating to privacy. Consumer subjects have the right to not see specific violating images on social media; the right to a certain level of protection against cyberbullying; the right to not be hacked. But workers face a completely different set of needs for protection because the power relation is entirely different. Workers' data is collected and utilised by companies to decide who we 'are', to decide whether we are talented, to check on our progress, productivity, sick leave, whether we met targets or not. These methods as well as other surveillance protocol allow interpellation of our profiles to aid decisions about us, about the level of risk we as workers pose to the company, often without our participation, or knowledge, and in ways that Althusser (1970) could only have imagined.

A good example for how power relations between workers and bosses in the algorithmic employment relationship is seen in the context of a platform taxi workers being deactivated, a situation whereby their device is switched off for numerical reasons such as if they do not take enough passengers or their customer ratings have reduced (Woodcock, 2021). The problem with this algorithmic decision is that it eliminates qualitative dimensions of human decision-making, where a taxi driver may decide not to pick up a passenger for all sorts of reasons. They may decide to take a break due to being overly tired, to eat a meal or to otherwise carry out human activities of necessity. The platform has no judgement capabilities around *reasons* for breaks, even where occupational safety and health is at risk, i.e., if a worker does not rest during a 12-hour period of driving. A passenger may give a taxi driver a bad rating simply because they could not find the driver in a busy street or when, in fact, the passenger's behaviour was not ideal, where someone intends to deflect responsibility.

Again, a rating system can only be presented seemingly objectively where the taxi driver data subject, therefore, is defined based solely on such datasets. In that light, an algorithm may allow management to perceive a taxi driver to be a 'risky' driver somehow and ultimately may deactivate him or her for a period, or forever. In this way, data takes on a life of its own. The use of data for objective decision-making was not, originally, seen to pose any kind of risk, where 'numbers don't lie', and the data may even now not be seen as possessing a subject position in and of itself. Even data itself appears to operate as a kind of subject. But the GDPR's algorithmic management component attempts to dampen this kind of decision-making and in the Spring of 2021, Case C / 13/696010 / HA ZA 21-81 in the Netherlands led to successful re-hiring of two taxi drivers who, the court decided, had been fired by algorithm.

While technology is perceived to hold risk within the AI Act, the conception and judgement of what precisely constitutes 'risky' behaviour and 'risky' work environments does not emerge with such precise categorisation. Worker extremes of all kinds can apparently pose a threat, or create a negative *risk*, for employers. The struggle between capital and labour oscillates around these perceived risks, where the risks that work and work expectations for workers is often far less considered than their risks of behaviour or actions taken by their counterparts, or their employers. Parameters are defined for what is 'too much' to be considered permissible for worker behaviour or expectations of workers without worker participation are not balanced with the consideration of what is 'too much' in terms of employer surveillance and increasingly minute judgement of work itself. In these contexts, the possibilities for discrimination and unconscious bias are enormously exacerbated, but give some kind of credibility for data collection, processing and usage in workplaces where collection becomes increasingly possible as workers work from home using IT systems.

On the other hand, we, as consumer data subjects, are aware that the large corporations GAFAM use our data constantly, where our profiles are laden with targeting based on data accumulation. We probably do not feel entirely exploited because we can use services such as social media platforms in exchange for mass personal data collection. However, the advantage of the trade-off between data sacrifice and the use of 'free' services in the digitalised world is less and less clear to people (Véliz, 2020: 157). Further to the increasing discomfort with what may feel like hostile data acquisition, datafied subjects are not equal nor identical in reasons nor social and economic positions in data affordance. Online self-branding is symptomatic of the fluctuating exchange rate within the attention economy, where subject formation has a value and as a result, the location of agency in subjectification is different depending on subject intention and due to the scale of audiences/customers online. While a lot of innovation, start-up and hackerspace enthusiasm for the seeming radical democratic potentials for self-expression and self-formation

offered by the internet at its nascence has been entirely drowned out by a venture capitalist revolution and corporate monopolisation of networking platforms (Drakopolou et al., 2016). Facebook, for example, was originally thought to hold the potential for community-building more than as a vehicle used for proprietary companies and advertisers that it increasingly has become, where people's data is used to further the interests of capital rather than necessarily their own interests. Nonetheless, Facebook, Twitter, Instagram and YouTube have made online self-branding, self-image-making, self-promotion and self-authorship possible and nearly a requirement for most public figures and celebrities (Duffy & Pooley, 2019).

A specific type of celebrity worker is emerging, the 'influencer', where competition for the *most authentic authenticity* is oddly rampant. This new genre of celebrity fits the 'idols of consumption' frame, chasing a 'contemporary valorisation of digital fame' (Duffy & Pooley, 2019) that harks back to Lowenthal's mass idols thesis from 1944. These new idols are of course themselves workers, within the immaterial labour frame (Lazzarato, 1996) and rely on an attention economy (Simon, 1969 as cited in Simon 1971; Bueno, 2017) for valorisation. This version of seeming 'employability' or 'clickability' anyway, is based on how authentic, as well as attractive or otherwise attention-worthy, they are, which is measured by numbers of followers and 'likes' for posts, data pools from which advertising companies can lucratively fish. So, there is a subject category collapse within 'employability' terms, where the relationship between consumer and worker is direct and directly quantifiable, where online observers are the new non-paying clients. Further to this, the worker as subject within these new types of economies and social relations is reliant on a specific version of time that's shared for the most part, across the human race, in ways that machines do not require. The quote from Bifo's 2011 *e-flux* paper is good, where he reminds us: 'do not forget that your brain functions in time, and needs time in order to give attention and understanding. But attention cannot be infinitely accelerated' (Berardi, 2011). Indeed, Berardi notes that the trends toward knowledge workers' interest in microdosing and amphetamines could be a result of workers being put in direct competition with machines.

But back to the discussions of how data subjects are not equal nor identical. The prosumer celebrity as an idolised influencer can potentially profit from advertising agency sponsorship, other industries' workers do not have a direct income possibility via the increase in data harvesting. While these categories are inherently imperfect due to the limitations of description in social science and humanities as well as legal studies apart from some of the definitions above; heuristically, they nonetheless are more granular than the all-encompassing 'data subject' evidenced in policy intending to protect the multiplicity of selves. My key argument is not that consumer subjects (as opposed to workers) are entirely protected by the GDPR as such, but given the history of protection in advertising and broadcasting law they are more protected than workers, simply because the supposed agency of a natural person in the consumer mode is definitive for capitalist sociality.

Consumers and workers are *subject to* quite different daily risks and antagonisms and *subjects within* variable social contexts and other rights, such as the right to personality. The questions around whether workers can build authentic selves stems from the Human Relations psychology of management school, where Mayo and colleagues argued that people can find pleasure in work and productivity to a point where even the work/life divisions may not be necessary at all. Context collapse, digital platforms as fashion templates, accelerated avenues for communication, and the sheer rise in audience scale for such phenomena within the contemporary era of digitalisation have meant that understandings of the boundaries between life and work are in danger of disappearing altogether. Nonetheless, material conditions within capitalism continue, where precarity has arguably replaced the once 'typical' employment relationship.

A stranger to ourselves

I do not accept, like Nietzsche's arguments in the *Will to Power,* that the subject contains a being in itself. Rather, data-based subjectification solidifies already-existing alienation and abstraction of labour power via numeration and quantification and limits agency for subject formation and subjectivation. If alienation exists and is possible, then we must assume and presuppose some kind of subject. The Nietzschean intervention is that the subject is a temporary formation within the flux of force, maybe like the flux of data creates the subject as a temporary granular formation which tomorrow can be and will be different. Indeed, datafication is a permanent process, constantly actualising by tracking, tracing, and controlling the subject, but within a cybernetic loop, producing a subjectivity that must also be self-recuperated. So, even where there can be datafication and profiling, without any acknowledgement of specific differences in power relations between various subject types, processes can weaken any capacity for bargaining for even basic rights, exogenously obtained, and secured.

Thomas Metzinger, a German neuroethics philosopher, describes core consciousness as that which creates a mental model of itself, which he calls the 'Phenomenal Self-Model' (PSM) (Metzinger 2003), which simultaneously holds a model of relations with others, called the 'Phenomenal Model of the Intentionality Relation' (PMIR). 'Self' in and of itself has never existed, Metzinger claims. But that does not mean that we do not have experiences of having a self, or being a self via, roughly, the experience of both PSM and PMIR. Consciousness relies on memory as well as the capability to predict the future or to anticipate future memories. N. Katherine Hayles, a feminist philosopher, intervenes in neuroscience debates from a largely new materialist lens with a rigorous discussion of nonconscious cognitions, indicating where this emerges in both human and non-human environments. Hayles writes that Damasio (2012) discusses the autobiographical self, which as Nelson (2003) indicates, is 'reinforced through the verbal monologue that plays in our heads as we go about our daily business; that monologue, in turn, is associated with the emergence of a self-awareness of itself as a self' (Hayles, 2017: 9-10). *Technical* cognition, or the level of supposed consciousness achieved by machines via machine learning and pattern recognition, is usually compared with the human 'operations of consciousness', because machines are seen to perform better than humans at specific tasks that apparently can be translated into cognition and consciousness. I agree with Hayles' scepticism of technical cognition but am still reticent about the claims that consciousness is the main thing that separates the human from other life forms. Indeed, the anthropocentric projection puts us in the prime position holder or possessor of consciousness, despite signs of animal and other cognitions which the cyberneticians posit.

Subjectivity, anyway, does not have one definition. As stated, questions of the subject drive a lot of Western philosophical enquiry. Communications and media theorists have talked about 'deep mediatization', building on Berger and Luckmann's 1960s research which indicates that:

> The most important vehicle of reality-maintenance is conversation. One may view the individual's everyday life in terms of the working away of a conversational apparatus that ongoingly maintains, modifies and reconstructs his subjective reality… (Berger & Luckmann, 1966: 152)

Andreas Hepp and Nick Couldry (2016) describe a 'materialist phenomenology of the digital world' whereby the social world ideally remains accessible to people by virtue of our own understandings and interpretation as mediatisation becomes increasingly pervasive, where there are real possibilities for collective becomings, and in that sense, possibilities

for empowerment in neoliberal enclosures. Crushing the human nomad condition and the potential for modalities discussed by Braidotti, where we 'live in permanent states of transition, hybridisation and nomadic mobility, in emancipated, post-feminist, multi-ethnic societies with high degrees of technological mediation which, however, have not ensured justice for all, or resolved enduring patterns of inequality' (2013: 1; also see Braidotti, 2002, 2006), the intensification and normalisation of the use of worker surveillance electronic performance monitoring technology in workplaces has been made even more evident in the context of the global pandemic. The alienation and abstraction of work resulting, require new lines of questioning and new analyses. Data, likewise, are not neutral entities that magically derive profiles that can be relied upon and cherished as true and accurate representations of ourselves. Indeed, the concept of 'subjectivity' is one of the most discussed in philosophical circles. So, what is needed, is a better investigation of the nature of the information that is generated by, and about, workers, and what happens to that data, in ways that become part and parcel to people's subjectivities.

Subject formation: Will numeration replace text?

The pursuit of datafication is defined as 'the process of rendering into data aspects of the world not previously quantified…. Not just demographic or profiling data but also behavioural metadata' (Kennedy et al., 2015: 1). This definition does not precisely capture my argument. I am arguing that the process of data-based profiling of humans is now carried out by other humans *based on* that process of rendering into data aspects that were not necessarily coded or recorded and quantified into data, which is expected to, in some way, be, or become meaningful and defining of the subject.

These processes of numerical delineation are beginning to replace textual hegemony. Operationalising a Gramscian definition, datafication of subjects may overcome the historical textual dominance for subject formation, which was based on language and communication, preceding the so-called corporeal turn I have written about elsewhere (2019), where the cultural era was seen to have been too reliant on text and traditional language, where contemporary social relations are increasingly dependent on symbolic languages of algorithm and coding alphabets. This is a different argument from those of Hegel's phenomenology of Spirit; and the ideas of Lumann and Du Bois as discussed by Schalk (2011) where mass media has had an impact on consciousness, self-reference and other-reference. Schalk argues that this binary is too limiting and that a third opposition of 'other-self' and 'self-mediation' is needed for better conceptualisations of otherness and of self/other relations. While that may be possible for some types of subjects, I want to argue that the worker cannot be conflated with other subjects.

Indeed, the discussions I have identified do not take the data subject in a power relationship with the already existing materialist present. Research within what is called the corporeal turn was argued to advance or overcome/end decades of media studies and social theory that focussed on text, which cleared the intellectual terrain for new materialisms (Coole & Frost, 2010) and agential realism (Barad) where bodies and materiality returned to thinkers' drawing boards. The 'posthuman' thesis is important to pursue lines of questioning around machinic agency and our role in the world (Haraway, 1991; Mitchell, 2003). I argue that arguments for the post-human and discussions of a post-work future are premature because we have not come to terms with text's arriving antithesis: numeration. While it has been thought that the capacity for human subjectivity rests on 'consciousness, universal rationality, and self-regulating ethical behaviour' (Braidotti, 2013: 2) and the 'other' defined as a 'negative and specular counterpart' (*Ibid*.), the portrayals of the

same have been dependent on textual and image representation. The competence for symbolic reasoning that becomes language and text cannot be separated from our bodies, however, reflecting a 'fundamental duality of being human: we are at once embodied and symbolic' (Tufekci, 2017: 862). Digital technologies have transformed our capacity for, and agency in, subjectivity and subjectification in a number of ways, from the curation of the self via social media platforms to a sense of a distributed, expansive self with multiplicities and becomings as mediated and advanced via what Couldry and Hepp call 'deep mediatisation' (2016), where human and machine agency become ontologically entangled (Beer, 2013).

For me, the most important point in critiquing current data regulation is that, rather than allow for sufficient protection and privacy, there are significant emerging obstructions already to becoming-human, to enunciation, to affective subjectivation. Ideally, my praxis in identifying the weaknesses in current policy can help us formulate alternatives for the emergence of sustainable subjects, where we may be in a position to 'enact a vision of the subject that encompasses changes at the in-depth structures' (Braidotti, 2014: 181), identifying collective intelligence and collective emancipations. The idea of the data subject begins well enough because there appears to be a chance to put the focus on people and protections for basic social justice; rather than a focus on machines, technological development, improvements of systems or organisational processes, as is often seen in law. However, when we begin to interrogate or problematise the ways that a data subject will experience aspects of their relations in the world, where for example, a consumer has very different personal stakes than both a worker and a citizen, we realise that human data and privacy protections such as the GDPR do not go far enough.

That being said, I do not have an immediate solution for how to rewrite regulation to accommodate modalities of data subjects. The latest trend in technology legislation, such as seen in the AI Act draft, is to outline judgments of perceived risks, as discussed in the previous section. Historically, people are the agents of risk, where a trade unionist might be risky, and there may be signs that a worker is becoming increasingly active in political work. Where judgements of risk are now being placed on technology directly, risk does not seem to be placed on users of the technology where the user is the company, at least as defined within the current AI Act draft.

	Loss of livelihood	**Psychosocial violence**	**Exploitation**	**Deperson-alisation**	**Algorithmic management**
Consumer	no	no	no	no	no
Worker	yes	yes	yes	yes	yes

Table 1: Data subjects: Subject *to*

	Access to data	**Voice**	**Dignity**	**Right to personality**	**Social security**
Consumer	yes	yes/no	yes	yes	n/a
Worker	?	?	?	?	?

Table 2: Data subjects: Subject *within*

	Surveillance	Possibility for consent	Discrimination	Hierarchies
Consumer	x	x	x	x
Worker	?	?	?	?

Table 3: Data subjects: Subjects *of*

There are distinctions and protections made for workers within the GDPR and the AI Act as I have outlined, but they are consistently weak. Indeed, worker protection tends to be left up to hiring institutions and organizations and their respective worker representative groups, such as trade unions which have variable strengths in various countries. As indicated in the Tables, workers are 'subject to' (Table 1) the risk of the loss of livelihood, psychosocial violence, exploitation and depersonalisation resulting from algorithmic management; where the context for these limitations mean we see that subjects exist 'within' (Table 2) environments where they do not necessarily have access to data, where their voice, dignity, right to personality and access to benefits such as social security, upon which decent work relies, is never secure. Adding to this, worker data subjects are subjects of surveillance, where consent is probably simply not possible, and where discrimination and hierarchy are ongoing (Table 3). So again, these differentials mean that privacy and data protection regulation today cannot fully be applicable for all data subjects, given the severe limitations.

4 Discussion and conclusions

Sceptics have already warned that the GDPR and the AI Act proposals do not go far enough to protect people. Digital intermediaries' use of data using a mixture of both legal and illegal activity is common and is very hard to trace. Patterns of collection can create stress for data subjects, rather than just one-off tipping points, which do not reflect the way real life operates. Veale and Zuiderveen Borgesius (2021) argue that the AI Act does little to improve on existing consumer, data, privacy, and technology laws, particularly with regard to protections for data subjects (who as I have stressed, are not named as such in the Act). While the rights of the data subject enjoyed attention (albeit quite briefly for workers) within previous legislation such as the GPDR, this subsequently went missing. Of course, AI augmented technology is perceived to hold levels of risk within the AI Act, as mentioned, but the conception and judgement of what precisely constitutes 'risky' implementation is not altogether clear. There is no discussion of 'risky' work environments, nor how management or even workers' activities might be considered as risky. Working data subjects are the most vulnerable (amongst non-clarified characteristics outside those which are protected), they are still least protected in this emerging draft legislation. As mentioned above, while there are some inroads for protections of the data subject in the GDPR, there is already not enough finessing in recognising the differences between the various subject parameter. The working data subject is not adequately protected with regards to data collection and usage.

Whenever limits are imposed on human subject-formation, there are real dangers of social damage, and thus, the application or use of data to identify subjects and the resulting processes of data 'subjection' and 'subjectification' requires investigation, urgently, as new policies are being authored to manage new technological interventions into organisations, such as AI. Perhaps we should speak not of a 'data subject' but of the *datafied*

subject, where power relations surrounding new subjectifications may mean we become strangers to ourselves, where people's subjection, as described by Foucault in his later works (1982), is such that the only subjective identity we are permitted (such as the 'employable' subject I have discussed (Moore, 2010), is that which is codified and collapsed, where others have more power to depict our supposed true selves than we have, even in cases where the subjected cannot depict who that 'other', is.

This article has argued that there is a cognitive distortion, if not cognitive error, in attempts so far to regulate privacy and data protection as it applies to workplaces and workers, in part due to the rise of the sphere of algorithmic management and human resources analytics, because of a homogenising nature in depicting the 'data subject'. Research that finds AI and algorithms to be discriminatory is now well known (Williams et al., 2018; Ajunwa, 2020; Köchling & Wehner, 2020). Black box processes lead to unclear outcomes of algorithmic processes, where even the algorithm's designer may not understand how the results have come about (Ajunwa, 2020; Pasquale, 2016). However, while the delineations in protected characteristics[8] which are protected in the GPDR are necessary and correct, they are not enough. There is insufficient delineation *beyond* protected characteristics to capture what is at stake for workers in new digitalised work relationships and conditions. Other law will have to be applied to provide better protections for workers. While not perfect, German labour law not only allows for co-determination but also protects the right to personality (Moore, 2020a). The problem is not that existing data protection and privacy policy does not provide any protection for anyone nor protections of specific characteristics, but that a one size fits all category for a human cannot, and will not, protect workers from the looming potential degradation and destruction of the employment relationship in several important ways, given workers are *subject to*, *subjects of,* and *subjects within* quite different pressures and power relationships than consumers as well as other types of subjectivities.

To come to some conclusions, and in parallel with the lines of argumentation that algorithms can result in discriminatory solutions (O'Neil, 2018, 2020) in order to resolve some of these issues, in fact, *more* discriminatory parameters within current data protection, privacy and AI regulation would be quite useful, which could help to provide better protections for specific types of a data subject, with better granularity, with better considerations for how policy might impact specific categories of people or categories *within* people, given a worker, a consumer and a citizen simultaneously house the same body. Policy and policymakers must 'back up' and stop allowing the technological tail to wag the dog, where assumptions about technology and even an ascription of subject status to data itself of risk, often works to define policy, rather than the other way around. Further to this, there are other laws that must be used to protect workers that go beyond privacy and data protection such as in labour law (Moore, 2020a).

his piece has first assessed the limitations of the concept of the data subject as presented within recent regulations including the GDPR and the AI Act. Then, I have laid out some ways to think about subjectivity, where subjection is the dominant model for human relations today, where the conflation of more than one subject positionality into one regulatory concept is evident. While there are very good arguments indicating that human data ownership will enhance agency (Powell, 2021; Pybus et al., 2015), my argument has so far been that the subject in capitalism is not liberated sufficiently to find complete emancipation or even protections in the current data and privacy regimes provided by policy. The

[8] Protected data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; and data concerning a person's sex life or sexual orientation.

act of identifying a data subject within regulation could have a positive effect, i.e., to allow regulators, authorities, and technology users and providers, a way to think about *who, exactly, is to/should be protected* and *how*, but as it stands, there is far too little discrimination across subjects. Lazzarato makes some insightful comments around capitalism which he talks about as a 'war machine', where legal and institutional apparatuses are built in ways that consolidate existing power structures and relations via governing the 'divisions of sex, race, and class, guarantors of the enslavements and subjugations implied by these divisions' (2021: 166). This important autonomist goes on to note that 'subjectivities choose, make decisions, but these decisions and these choices are meant to establish or re-establish the functioning of the machine' (*Ibid.*). Lazzarato (2021) points out that the paradox of elite-defined subject definition becomes evidenced during a crisis, when a closing of multiplicities constitutes an explicit attack on subjectivation and emancipation. While the current piece has not been written during a period of economic crisis as such, the apparatus has already been set and is designed precisely in this manner, a strategy of obstruction and a war of position.

To conclude, I would like to note that alongside the failure of sufficient nuance in a data subject positioning to identify how workers' struggles differ from consumers' struggles, there is also insufficient attention placed on workers' potential roles in decision-making for all data integration into workplaces. Organisations have written data codes of conduct such as the International Labour Organization in 1997 (ILO, 1997), which was an early intervention outlining how data should and should not be used/gathered/processed and so on, with an appropriate emphasis on workers. These important ILO principles should be updated to reflect the advancements in technological surveillance in workplaces and societies. Co-determination is another important route. Information about personal and privacy protections relating to how data is gathered, processed, used, and stored, should be disseminated by DPOs, whose roles are to some extent, discussed within the GDPR, but whose responsibilities should be better defined, so that explicit integration with worker representative communities could be made possible (Moore, 2020a).

Data construction of subjects, and our subjection via profiling in people analytics and human resources processes must be problematised and the question specifically asked: what happens to our subjectivities within the line of communication, whether with a DPO or with a company's platform interface? What happens when data is used to formulate and portray specific profiles and portrayals of data subjects via profiling and other means and when the social relation dimension of the employment relationship is absented? Is this a process of subject, or rather, object formation? Is this a process of control, where workers have depleted agency, where rather than machine risk, profiling and other data usage is designed to identify risky subjects? Who are we 'becoming'? Are we seeing data becoming a subject in itself, where we have begun to even interpellate data with decision-making qualities? As we experience continued precarity of working conditions and struggles for basic rights at work, the question of emancipation depletion is very real and increasingly vital. Who now has the right to 'enunciation', or the right to formate the self, the right to subjectivity and in that context, agency? This paper has attempted to demonstrate the ontological and epistemological problems with the very concept of the 'data subject', which itself makes it difficult to see how its use in data and privacy policy can ever lead to full protections for people, as we become strangers to ourselves.

8 References

Abraha, H. (2022). EU Member States' Use of Art 88 GDPR. Talk for Algorithms at Work. Oxford Law Faculty 03/03/2022.

Adams-Prassl, J. (2020). What if your boss was an algorithm? The rise of artificial intelligence at work. Comparative Labor Law & Policy Journal, 41(1), 123 – 146.

Ajunwa, I. (2019). Algorithms at Work: Productivity Monitoring Applications and Wearable Technology. St. Louis University Law Journal, 63(21), 21-54.
Ajunwa, I. (2020). The ‘black box’ at work. Big Data & Society. 7(2), 1-6.
Alizart, M. (2020). Cryptocommunism. Cambridge, UK: Polity Press.
Althusser, L. trans. by B Brewster (1970). Ideology and Ideological State Apparatuses. La Pensée.
Amoore, L. (2013). The politics of possibility. Durham, NC: Duke University Press.
Andrew, J. and Baker, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism Journal of Business Ethics. 168, 565 – 578.
Avila Negri, S. M. C. (2021). Personhood in robotics and artificial intelligence. Hyupothesis and theory argticle, Frontiers in Robotics and AI. 23 Dec 2021, Retrived from https://www.frontiersin.org/articles/10.3389/frobt.2021.789327/full
Beer, D. (2013). Popular culture and new media: The politics of circulation. Basingstoke: Palgrave Macmillan.
Berardi, F. (Bifo) (2011). Time, Acceleration, and Violence. e-flux Journal 27, Retrieved from https://www.e-flux.com/journal/27/67999/time-acceleration-and-violence/
Berger, P. L. and Luckmann, T. (1966). The Social Construction of Reality: A Treatise in the Sociology of Knowledge. USA: Penguin Books.
Berry, D. (2014). Critical theory and the digital. London: Bloomsbury.
Bloom, P. (2019). Monitored: Business and Surveillance in a Time of Big Data. London: Pluto Press.
Botanski, L. and Chiapello, E. (2007). The New Spirit of Capitalism. London: Verso.
Braidotti, R. (2002). Metamorphoses. Towards a Materialist Theory of Becoming. Cambridge: Polity Press/Blackwell.
Braidotti, R. (2006). Transpositions: on nomadic ethics. Cambridge: Polity Press.
Braidotti, R. (2014). Writing as a nomadic subject. Comparative Critical Studies, 11(2-3), 163–184.
Braidottti, R. (2013). Posthuman Humanities. European Educational Research Journal 12(13) 1–19.
Bueno, C. C. (2017). The attention economy: Labour, time and power in cognitive capitalism. Maryland: Rowman and Littlefield.
Butler, J. and Spivak, G. (2007) Who sings the nation state? Calcutta: Seagull.
Coole, D., Frost, S. (2010). New Materialisms: Ontology, Agency and Politics. Duke: Duke University Press.
Cornell Legal Information Institute (2022a). Definition of natural person. Open Access to Law. Retrieved from https://www.law.cornell.edu/wex/natural_person
Cornell Legal Information Institute (2022b). Definition of artificial person. Open Access to Law. Retrieved from https://www.law.cornell.edu/wex/artificial_person
Cornell Legal Information Institute (2022c). Definition of consent. Open Access to Law. Retrieved from https://www.law.cornell.edu/wex/consent
Couldry, N. and Hepp, A. (2016). The Mediated Construction of Reality. Cambridge: Polity Press.
Couldry, N. and Powell, A. (2014). Big data from the bottom up. Big Data and Society,1(1): 1.5.
Deleuze, G. (1995) Negotiations, 1972 – 1990. Columbia: New York University Press.
Deleuze, G., Guattari, F., & Massumi, B. (1987). A Thousand Plateaus: Capitalism and Schizophrenia (2nd ed.). University of Minnesota Press.
Drakopoulou, S., Grossman, W. M., Moore, P. (2016). The campaign for digital citizenship. Soundings, 2016(62). Retrieved from https://journals.lwbooks.co.uk/soundings/vol-2016-issue-62/abstract-7500/
Duffy, B. E. and Pooley, J. (2019). Idols of Promotion: The Triumph of Self-Branding in an Age of Precarity. Journal of Communication, 69(1), doi:10.1093/joc/jqy063
European Commission (EC) (2021). AI Act draft Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts {SEC(2021) 167 final } - {SWD(2021) 84 final} - {SWD(2021) 85 final} (Brussels, 21.4.2021). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
European Data Protection Board (EDPB) (2020). Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1. Adopted on May 2020. Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
Evans, L. and Kitchin, R. (2018). A smart place to work? Big data systems, labour, control and modern retail stores. New Technology, Work and Employment, 33(1), 45 – 57.
Foucault, M. (1982). The Subject and Power. Critical Inquiry, 8(4), 777–795.
Fuchs, C. (2011). Web 2.0, Prosumption and Surveillance. Surveillance & Society, 8(3): 288 – 309.
GDPR Article 4.1 (2020). Definitions. Retrieved from https://gdpr.eu/article-4-definitions/
GDPR Article 6 (2020). Lawfulness of processing. Retrieved from https://gdpr-text.com/read/article-6/
Gramsci, A. (1971). *Selections from the Prison Notebooks*. Translated and Edited by Q. Hoare and G. N. Smith. New York: International Publishers.
Gunkel, D., Coeckelbergh, M. and Gerdes, A. (2022). Should Robots Have Standing? The Moral and Legal Status of Social Robots. Retrieved from https://www.frontiersin.org/research-topics/17908/should-robots-have-standing-the-moral-and-legal-status-of-social-robots#articles
Haraway, D. (1991). Simians, cyborgs, and women: The reinvention of nature. London: Free Association Books.
Hayles, N. K. (2017). Unthought: The Power of the Cognitive Unconscious. Chicago: University of Chicago Press.
Institute for the Future of Work (2020). Artificial intelligence: Assessing impacts on equality. Retrieved from https://www.ifow.org/publications/artificial-intelligence-in-hiring-assessing-impacts-on-equality
International Labour Organization (ILO) (1997). Protection of workers’ personal data. Retrieved from https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_107797/lang--en/index.htm
Introna, L. D. (2011). The enframing of code: Agency, originality and the plagiarist. Theory, Culture & Society, 28, 113–141.
Irish Data Protection Commission (2019). Data Protection Statement. Retrieved from https://www.dataprotection.ie/en/about-our-site/data-protection-statement
Jack, A. (22.09.2021). Growth of Staff Monitoring Software Stokes Debate over Rights and Morals. Financial Times, Financial Times Special Report: Future of the Workplace. Retrieved from https://www.ft.com/content/ab61541a-b6c1-45cb-b9ad-f338ec08cf61
Kennedy, H., Poell, T. and van Dijk., J. (2015). Data and agency. Big Data & Society, 3(1-2).
Kim, S. O.-V-C (2011). Critique and Subjectivation: Foucault and Butler on the Subject. Actuel Marx ,49(1), 148–161.

Köchling, Al. and Wehner, M. C. (2020). Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. Bus Res, 13(3), 795-848.
Lazzarato, M. (1996). Immaterial Labour. In: Virno, P. and Hardt, M. (eds.). Radical Thought in Italy: A potential politics. Minnesota: University of Minnesota Press. 133-147
Lazzarato, M. (2021). Capital Hates Everyone: Fascism or Revolution. California, USA: semiotext(e).
Lilkov, D. (2021). Regulating artificial intelligence in the EU: A risky game. European View 20(2), 166–174.
Lordon, F. (2014). Willing Slaves of Capital. London and New York: Verso.
Mackenzie, D. (2001). Mechanizing Proof. Computing, Risk, and Trust. Cambridge, Mass.: MIT.
Metzinger, T. (2003). Being no one: The self-model theory of subjectivity. Cambridge, Mass.: MIT.
Mitchell, W. J. (2003). Me++: The cyborg self and the networked city. Cambridge: MIT Press.
Moore, P. V. (2010). The International Political Economy of work and employability. London: Palgrave Macmillan, International Political Economy Series.
Moore, P. V. (2019). The Quantified Self in Precarity: Work, Technology and What Counts. London: Routledge.
Moore, P. V. (2020a). Data Subjects, Digital Surveillance, AI and the Future of Work. Brussels: European Parliament Science and Technology Office. Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)656305
Moore, P. V. (2020b). The mirror for (artificial) intelligence: In whose reflection?, for Special Issue Automation, AI, and Labour Protection, V. de Stefano (ed.), Comparative Labor Law and Policy Journal, 41(1): 47-67.
Mueller, G. (2021). Breaking Things at Work: The Luddites are Right about Why You Hate Your Job. London and NY: Verso.
O'Neil, C. (2016). Weapons of Math Destruction. USA: Crown.
O'Neil, C. (2020). Algorithmic Stakeholders: An Ethical Matrix for AI. Data IKU Blog. Retrieved from https://blog.dataiku.com/algorithmic-stakeholders-an-ethical-matrix-for-ai
OECD (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1
Ogriseg, C. (2017). GDPR and Personal Data Protection in the Employment Context. Labour and Law Issues, 3(2), 2421-2695.
Pakes, A. (2020). Data Protection Impact Assessments: Guide for union representatives. Prospect. https://d28j9ucj9uj44t.cloudfront.net/uploads/2020/12/prospect-dpia-workers-guide.pdf
Pasquale, F. (2016). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard: Harvard University Press.
Purtova, N. (2021). From Knowing by Name to Personalisation: Meaning of Identification Under the GDPR. Available at: https://ssrn.com/abstract=3849943 or http://dx.doi.org/10.2139/ssrn.3849943
Pybus, J., Cote, M., & Blanke, T. (2015). Hacking the social life of Big Data. Big Data & Society, 2(2), 1-10. Retrieved from https://doi.org/10.1177/2053951715616649
Rani, U. and Furrer, M. (2021). Digital labour platforms and new forms of flexible work in developing countries: Algorithmic management of work and workers. Competition and Change, 25(2): 212 – 236.
Rosenblat, A. and Stark, L. (2016). Algorithmic labor and information asymmetries: A case study of Uber's drivers. International Journal of Communication 10, 3758–3784.
Schalk, S. (2011). Self, other and other-self: going beyond the self/other binary in contemporary consciousness. Journal of Comparative Research in Anthropology and Sociology, 2(1), 197 – 210.
Simon, H. A. (1971). Designing Organizations for an Information-Rich World, in Martin Greenberger, Computers, Communication, and the Public Interest, Baltimore, MD: The Johns Hopkins Press, 40–41.
Thompson, P. (2003). Fantasy Island: A labour process critique of the 'age of surveillance'. Surveillance & Society, 1(2), 138–151.
Trades Union Congress (2020). Technology managing people: The worker experience. London: Trades Union Congress.
Tufecki, Z. (2014). Are we all equally at home socialising online? Cybersociality and evidence an unequal disdain for digitally mediated sociality. Information, Communication and Society, 17(4), 486 – 502.
Van Dijck, J (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. Surveillance and Society, 12(2), 197 – 208.
Veale, M. and Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence act. Computer Law Review International. Retrieved from https://osf.io/preprints/socarxiv/38p5f
Véliz, C. (2020). Privacy is Power: Why and How you should Take Back Control of Your Data. London: Penguin Random House.
Wachter, S. (2019). Data protection in the age of Big Data - Europe's data protection laws must evolve to guard against pervasive inferential analytics in nascent digital technologies such as edge computing. Nature Electronics, 2(1) 6-7.
Whitehead, N. L. and Wesch, M. (2012) Human no more: Digital subjectivities, unhuman subjects, and the end of anthropology. Colorado: University Press of Colorado.
Williams, B. A., Brooks, C. F., Shmargad, Y. (2018) How algorithms discriminate based on data they lack: Challenges, solutions and policy implications Journal of Information Policy, 8, 78 – 115.
Woodcock, J. (2021). The Limits of Algorithmic Management: On Platforms, Data, and Workers' Struggle. South Atlantic Quarterly, 120 (4), 703–713.
Zuboff, S. (1988). In the age of the smart machine: The future of work and power. New York: Basic Books.
Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power. London: Profile Books Ltd.