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

Accepted for publication in Maurizio Atzeni, Dario Azzellini, Alessandra Mezzadri, Phoebe Moore, and Ursula Apitzsch (eds.) 2023. Handbook of Research on the Global Political Economy of Work.

Problems in protections for working data subjects: The social relations of data production[1]

Phoebe V Moore

Abstract: 'Problems in protections for working data subjects: the social relations of data production' argues that existing AI and data and privacy regulation does not sufficiently provide protections from harm in the context of data extraction and mining. This is because the approaches taken are individualist in relational positioning and do not take into account differences across data subject types. The argument updates legal philosophical arguments rooted in propertarian and identitarian assumptions for how data harms can be prevented, arguing that what is needed is a discussion of the social relations of data production and the portrayal of a constellation of power relations rather than identifying a data subject as suspended in midair.

1. Introduction

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.[2] Natural persons, who are humans, are identifiable 'data subjects' as labelled within data privacy law e.g., the General Data Protection Regulation (GDPR). Technically, data subjects 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)

Viljoen (2021) discusses 'propertarian' and 'dignitarian' approaches, from a legal perspective, which aid in thinking about the harms that data collection and usage pose for working data subjects in the context of regulation. The propertarian reform methodology sees data as property and/or labour and sees personal ownership of data as a solution to the potential harms this introduces. The dignitarian reform approach sees a data subject's right to self articulation in a state of erosion and the threat to autonomy can only be resolved by revisiting and re-establishing fundamental rights.

[1] Moore, P. V. (2023). Problems in protections for working data subjects: The social relations of data production. in Atzeni, M., Mezzadri, A., Azzellini, D., Moore, P. V. , and Apitzsch, U. (eds.) (2023). *Handbook of Research on the Global Political Economy of Work* (Edward Elgar).

[2] 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).

However, of these two approaches, neither properatian nor dignitarian is sufficient for addressing datafication issues emerging in the realm of social relations, which are involved in data collection (extending beyond the bilateral notion of consent and other wider relations we will discuss). Kennedy (et al) describe datafication as a 'process of rendering into data aspects of the world not previously quantified' (Kennedy, Powell and Van Dijk, 2015), referring to Van Dijck's warnings around dataveillance (Van Dijck, 2014) and related power relations. Rather than putting the focus on the use of data for worker surveillance and the potential harms that emerge as I have done in other work (Moore, 2020a), this chapter looks at recent data protection and technology regulation to identify to what extent it relies on unworkable data harms prevention or whether it has any relevance for the same given policies' epistemological positionings. Data subjects at work do, or technically should, have specific and known bilateral relationships with management and with data protection officers, but data subjects' relationships go far beyond this bilaterality. All productive forces exists within an ecology of 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 elsewhere (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.

Increasing the rights and protections of individuals and putting more obligation onto organisations to store data properly and to give people access to and ownership of data, which recent data regulation offers, sound wonderful and useful; and the idea that there can be better data and privacy protections for workers who should be able to use data to find meaning and self fulfilment is altogether progressive.

Datafication is a problem for individuals not because of surveillance only, but also because it can erode the right to self formation in a Foucaultian sense. But even the concept of self-formation and subjectivation is problematic if it focusses on an individual as the primary and sole unit of analysis. Current data and privacy protections policy largely omits the recognition of a key point about humanity within the conditions of capitalism, which is that we operate based on social relations. Indeed, data collection *is a social relation*, and the related power dimensions of social relations absent in the propertarian and dignitarian reform modes of analysis which dominate data protection epistemologies.

This chapter addresses the problems with policies intending to defend data subjects today, taking note of these problems. First, I identify how the data subject is articulated in data protection and technology policies focussing on the GDPR and the AI Act. European policy is the most liberally progressive in their properaterian and dignitarian gestures. However, protections of consumers and possibly citizens are more plausible results from these policies than protections of working data subjects. Without due consideration of the social relations of data production and related power relations as they differ across types of data subjects, policy will fall short of providing full protections for workers.

2. The data subject in policy

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). Nonetheless, 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'.

While the delineations in protected characteristics[3] 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). Here, I identify how the GDPR sets out to protect people from data harms with possible protections as well as significant limitations.

GDPR. The 'data subject' was originally termed as such within the 1995 Data Protection Directive which was reworked to become the Data Protection Act 1998 and then again reworked to become what we now know to be the GDPR. The GDPR is a propertarian policy, where subjects' rights to data is positioned as the answer to any perceived harm that might occur as data has become the 'oil of the digital era' (Economist, 2017).

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)

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)

[3] 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.

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. 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'.

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).

Individuals do not exist suspended in mid-air but are subjects within social relations, subject to, subjects of and subjects within a myriad context (Tables 1 – 3). 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. Worker data subjects are subjects of surveillance, where consent is probably simply not possible, and where discrimination and hierarchy are ongoing (Table 3).

So, the first problem with data and privacy regulation is that data subjects risk very different things depending on whether they are experiencing data extraction in the body of the worker, the consumer, the citizen, or another category. The social relations experienced by each have variable power aspects and bilateral tensions across subjects such as between manager and employee.

	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*

AI Act. While the GDPR explicitly discusses data subjects, the AI Act almost entirely overlooks this category. 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[4] draft is in circulation (in the second quarter 2022). The AI Act is digital single-market rather than human-focussed. It will require technology providers to inform users[5] 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. The 'data subject' concept, however, does not appear. This is problematic, since the concept of risk inherently alludes a social relation, where a harm can emerge. Liability questions also arise where blame and responsibility are also mostly missing.

The draft Act is oriented around technical approaches and company certification and liabilities rather than on the potential harms to data subjects. This significantly diverges from the GDPR's properetarian approach and indeed does not have a clear approach to data protection and privacy. The AI Act, however, advances 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.

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;

[4] 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).

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

- 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 traceability of data and documentation (EC, 2021, 3.3. Impact Assessment, 9).

3. Social relations of data production

Consent is a social relation. While a data protection office (DPO) is expected to hold a position to acquire consent with data subjects which would be a bilateral social relation, all data subjects have far more relationships with far more living human beings than with the DPO alone (Abraha, 2022), lending far more complexity to any notion or likelihood of bilateral consent. The GDPR requires a DPO to be appointed for any organisation with over 25 employees. This is an important position. The DPO should ideally 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.

'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 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[6]; 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 exist first and foremost between a wider social constellation of forces i.e., between management and a workforce, labour markets and governments and so on. So, for a data subject to have consciously made a decision - which is both genuine and informed, these power relations must be taken into account. 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 in their respective workplaces. While the sample was relatively small, the cameos presented in that policy report reflect the endemic lack of dialogue between workers and management around reasons for and the potential uses of personal data at work. 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 surrounding exploitation but have made some gesture of consent all the same (Gramsci, 1971).

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 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). The epistemological set of supposed choices between affective joy or sadness whether at work (or in the supermarket or a migration office), 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).

Consent is a (social) 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. This is a social relation necessary for production, however, it is difficult to understand how a data subject can be expected to provide consent, at all.

[6] Note Herman Melville’s parable where the worker the Bartleby the Scrivener, states ‘I would prefer not to’. While this story shows worker agency, in the end, the worker is put in prison and starves.

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.

4. Working (risky) data subjects

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).

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 (or doctor and patient, lecturer and student, and so on). 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. The concept of risk is part of an ecology of social relations, just as consent is.

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.

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.

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, and where the social relations of data production are power relations and occur in more than bilateral relationships, we realise that human data and privacy protections such as the GDPR do not go far enough. The AI Act, which is at the time of writing still undergoing consultation and amendements as led by the Internal Market and Consumer Protection committee, and the Civil Liberties, Justice and Home Affairs committee, holds some protections from the most risky applications of AI for consumers, workers and citizens and makes gestures

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 as well as those who suffer the harms emerging from such risks. But, as I have argued, profiling based on data collection at work can also be used to identify risky subjects e.g., someone involved in activism or 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.

5. Discussion and conclusions

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 which requires recognition of the sociality inherent to data collection and processing. Data is not only collected bilaterally, it rather occurs across modalities and locations and the impact that data extraction and mining of human goes far beyond individuals alone and therefore, properaterian and individuation approaches to data protection and privacy are insufficient for worker data subject protections.

The 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 recognition of the multiplicities of relations that data subjects have, beyond the bilateral relationship with a data protection officer, the abstracted relationship with the 'algorithmic boss' (Adams-Prassl 2020; Aloisi and De Stefano 2022). 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. The dangers of isolating a data subject to considerations of binary relations only, which the GDPR does, is the ongoing consolidation of the apparatus of capitalism which has already been set and is designed precisely in this manner. Much is needed to formulate a strategy of obstruction and a war of position.

Legal experts have already warned that the GDPR and the AI Act proposals do not go far enough to protect people (De Stefano, 2020). 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. 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 in subsequent European data law. AI augmented technology is perceived to hold various levels of risk within the AI Act, the conception and judgement of what precisely constitutes 'risky' implementation is not altogether clear. There is no discussion of 'risky' work environments, 'risky' social relations in terms of the employment relationship and surrounding tensions and impossibility for consent, nor how fragmenting a secure employment relationship itself might (should) be considered as risky for workers ourselves. Working data subjects are always already subjects in an unequal power relations, but we are still least protected in this emerging draft legislation.

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.

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).

This piece has first assessed the limitations of the concept of the data subject as presented within recent regulations. 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.

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?

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.

Aloisi, A. and De Stefano, V. (2022). Your boss is an algorithm: Artificial Intelligence, Platform Work and Labour. Oxford: Hart Publishing Bloomsbury.

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.

De Stefano, V. (2022). AI and digital tools in workplace management and evaluaction: An assessment of the EU's legal framework. European Parliamentary Research SEvice STOA P 729.516 May 2022. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729516/EPRS_STU(2022)729516_EN.pdf

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

Economist, The (2017). The world's most valuable resources is not longer oil but data May 6, 2017.Retrived from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

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.