BRIEFING
STOA Options Brief

European Parliament

Data subjects, digital surveillance, AI and the future of work

This Options Brief has been prepared alongside the report on 'Data subjects, digital surveillance, AI and the future of work', commissioned by the European Parliament's Panel for the Future of Science and Technology (STOA). The Brief provides first principles and policy options.

> *Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace (Data Protection Working Party 2002: 4).*

It is not extraordinary in itself that workers' activities are observed by management. Management want to know that workers are working, how well they are working, and how much to pay them. However, today, technological tools such as artificial intelligence (AI) can gather more and more data, and machine learning and algorithms allow computational processes to make seemingly autonomous decisions about workers, based on big data sets about them. Data protection regulation has been strengthened with the General Data Protection Regulation (GDPR), but companies' lack of due diligence has led to law suits and fines. Workers' data rights must therefore be protected, and this Policy Brief outlines first principles and policy options to achieve this.

Table 1 – First principles and policy options

First principles	Data protection and first principles, protection by design and default
	Proportionality, necessity, transparency
	Co-determination
	Prevention over detection
	Collective data governance
Policy options	Require union/worker involvement at all stages
	Introduce and enforce co-determination into labour law in all EU Member States
	Businesses to compile certification and codes of conduct
	Prioritise collective governance

This Brief looks at first principles for data protection and privacy at work and then proposes a clear list of policy options that EU Member States should take into account to ensure these principles are followed and enacted. Overall, companies and local government policy must prioritise interests of workers in a wider remit, i.e. protect workers against techno-stress and the psychosocial hazards created by data collection and tracking, and include worker representative groups at all stages.

1. First principles

Data protection and first principles, protection by design and default

This first principle is overarching, requiring the direct involvement of union representatives as full social partners in negotiations regarding necessity and proportionality, to decide whether implementation is necessary at all; in co-design and co-creation; and in meaningful involvement in the impact assessment and execution phases of any worker data collection and processing intervention. The principles involve: ensuring data transparency; meaningful assessment and discernment of the legitimacy of practices; accuracy, facilitated by checks on practice; both monitored and enforceable time-limits; and, importantly, the right for workers to explicitly control any device that will monitor their work, as well as to opt out. All of these principles must be both collectively decided and consented to by unions, as well as designed and implemented in partnership with workers' representatives. Workers' representatives must be appropriately trained, with expertise in data protection, and work alongside Data Protection Officers (DPOs)[1] to ensure these principles are met.

Proportionality, necessity, transparency

Precise identification of the necessity for technological tracking must be informed through negotiation as to what can be deemed proportional to workers' privacy, and must take their wider interests seriously. Privacy is more than an interest, it is a right. A whole range of interests surround and are entangled with aspects of privacy and these are at stake in the monitored workplace and space, making them relevant to discussions of necessity and proportionality. Privacy and related worker interests should be discussed and agreed in consultation and through collective bargaining with unions. All monitoring and tracking processes must be made transparent to workers, with DPOs and trained trade union representatives working together to agree on proportionality and necessity.

Co-determination

Co-determination is where workers sit on management boards and are directly involved in making decisions about changes to working conditions and business operations. Most of the European Union's (EU) post-Brexit Member States enjoy some kind of co-determination in state-run firms and the private sector. Those countries which do not enjoy the right to co-determination are: Belgium, Bulgaria, Cyprus, Estonia, Italy, Latvia, Lithuania and Romania. All EU Member States should implement some form of co-determination (also see 'policy options' below). In countries where co-determination rights exist, all data collection and processing activity must be co-determined. Companies and labour authorities must take note of the legal apparatuses in countries with co-determination rights and ensure adherence to them.

Prevention over detection

Data tracking systems in the health and safety remit should be designed to spot possible problems in advance, by ensuring correct procedures are followed, particularly when safety and health are at risk. Prevention is a better approach than solely detecting on-the-spot problems when they arise and then dealing with any aftermath when safety is compromised. However, for other identifiers gained from monitoring and tracking that occur in the human resources remit, the concept of 'prevention' is not as straightforward. A justification advanced for cameras that watch employees in retail has been to prevent

[1] The term 'Data Controller' refers to the institution or organisation that collects data. All Data Controller institutions are required to have an individual employee with the title 'Data Protection Officer', who audits and reports on compliance.

theft. A rationale for introducing backdoors for email and checks on computer usage has been to protect systems from security breaches. However, if there are ways to prevent such activities that do not involve constant filming of retail workers' activities or capturing every keystroke made by a worker, then the alternative analogue approach should be taken. In fact, in extending the concept of prevention, outright prevention of the adoption of technological tracking should be a viable option.

Collective data governance

The GDPR is written with the individual in focus. However, data collection operates at more levels than the discrete and the use of data collection impacts groups of all kinds, qualities and quantities, as well as individuals. Data governance should therefore be seen as a collective good, where all social partners must be involved. The bigger the dataset, the more powerful it is, because it can be used to train algorithms for decision-making with consequences at societal level. Responses to large data sets and their collection should therefore be collective, rather than individualised. Consent, however, is usually perceived to be a unidirectional arrangement and considered intrinsically impossible in the employment relationship. Nevertheless, in countries which enjoy co-determination rights, digital workspace transformations require negotiation and bargaining between workers and management to proceed and are therefore governed collectively, rather than relying on individual consent alone.

2. Policy options

Require union/worker involvement at all stages

Workers' interests should always be at the forefront of company approaches to privacy and data protection and worker representatives must be consulted when a new technology is considered for operations and analytics. The involvement of worker representatives at each increment of the life cycle of any technological tracking procedure is strongly recommended (see Table 2). The role of the DPO can be filled by an existing employee or partner, but it is advised that the DPO is provided with autonomy and legal protections, due to inevitable conflicts of interest. In addition to the DPO, a parallel worker representative, in the form of a union officer with expertise in data protection rights, should be appointed to carry out activities alongside the DPO, and with equal decision-making authority. The DPO and their union parallel must meaningfully communicate details of worker's rights to access; rectification; erasure; restriction of processing; data portability; and notification of explanation, particularly in the event of automated decision-making. Workers must be consulted if the Data Controller (usually the company or organisation) intends to disclose data to third parties.

Table 2 – Collective determination of data rights

Introduce and enforce co-determination into labour law in all EU Member States.

Building on the experiences and activities of union partners across the EU and the world, EU Member States should work to improve national collective bargaining rights and labour law through cross-border discussion and work to agree on best practices via Eurofound, with the emphasis on achieving co-determination rights which should be incorporated in all Member States. Correspondents from Member States plus Norway regularly report to Eurofound, proposing research questions that inform and establish comparative overviews and identify specific themes for large research projects, which should be about worker data protection and privacy in the GDPR era. Correspondents should also look at the successes among the cases across the EU and reported in the report on 'Data subjects, digital surveillance, artificial intelligence (AI) and the future of work'. Another good resource is the ILO's Protection of Workers' Personal Data Code of Practice of 1997. An updated framework based on this Code of Practice, prepared collaboratively with all social partners, as well as detailed reviews of existing co-determination and union

successes, are needed to cultivate cross-border awareness raising and local labour law and trade union coordination.

Businesses to compile certification and codes of conduct

To ensure full inclusion of employers in data tracking and processing activities as partners rather than just directors and managers, all DPOs should be proactive and include trade unions as well as employer associations. Indeed, to demonstrate good practice, and to ensure lawfulness and protection of workers' rights, DPOs should work with employer associations to write codes of conduct to accompany any system that processes data. This will ensure that employers understand the wider context within which their activities function and that consultation has operated with a wider inclusion of all social partners.

Prioritise collective governance

Companies and organisations which process large sets of data, process sensitive data or whose central function is to collect and process data, and all public bodies, are required to have a DPO. As outlined in the first policy option, a worker representative should also be assigned as a data rights steward and work in parallel with the DPO. To progress on the practicalities of collective governance, alongside the European Data Protection Board (EDPB) 2020 Guidelines on consent under Regulation 2016/679 (Version 1.1, adopted in May 2020), and given it is unlikely that collective governance can be achieved within the inherently unequal employment relationship, the concept of 'consent' must be entirely reconsidered. Along the lines of the updated EDPB Guidelines on consent, the:

> *…requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. (EDPB 2020: 6)*

While consent is only one of six criteria that may be selected by a company to identify the lawfulness of its actions, it is nevertheless worthwhile maintaining the issue of consent to data collection and processing on the agenda, particularly if co-determination is legislated following collective bargaining between employers and worker representative groups. Consent could ultimately take a different form to the present concept, and could be subject to an intellectual reappraisal, as well as redefined, to ensure that it is a meaningful when pursued via unions and a collective voice, rather than simply individually.

This document is based on the STOA study 'Data subjects, digital surveillance, AI and the future of work'. The study was written by Phoebe V Moore, University of Leicester School of Business, at the request of the Panel for the Future of Science and Technology (STOA), Scientific Foresight Unit, within the Directorate General for Parliamentary Research Services (EPRS), European Parliament. STOA administrator responsible: Mihalis Kritikos.

DISCLAIMER AND COPYRIGHT

stoa@ep.europa.eu (contact)

http://www.europarl.europa.eu/stoa/ (STOA website)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)