



Artificial Intelligence

Monitoring employee behaviour through AI

Employers already use various methods for monitoring employees and for a number of different reasons, from checking up on appropriate email and internet use to gathering information about productivity, reliability, employee interaction, location and health. In many ways, the issues are the same regardless of the sophistication of the technology used to carry out the monitoring and analysis of the results. There is no doubt that these tools can be very useful for employers wishing to identify inefficiencies in their business model and teams and AI can help bring speed, new insights and objectivity to this. However, assessing performance solely with cold hard data generated by technology or managing a remote workforce using AI based analytics at the expense of the human touch raises a number of legal issues.

The principal ones arise in the context of the European Human Rights Convention and data protection legislation. Excessive, unnecessary or unjustified monitoring will fall foul of both and proportionality will be key in determining the lawfulness of an employer's actions.



Human rights

The rights most relevant (and potentially at risk) in a monitoring scenario will be the right to private life and family life and the right to a fair trial (which might be engaged, for example, to consider whether evidence relevant to disciplinary proceedings was gathered lawfully). Employees have a reasonable expectation of privacy in the workplace although an employer can interfere with that right where it has legitimate grounds and it uses proportionate means to do so. Proportionality will involve looking at alternatives to achieving the employer's aim which are less intrusive and do not curtail the right to privacy. Being clear with employees about what they can and cannot expect regarding privacy in the workplace and the wider employment relationship generally will also be important.



Data protection

Data protection has taken centre stage this year with the EU General Data Protection Regulation (the 'GDPR'). Monitoring workers will involve processing their personal data and engage the employer's obligations as a data controller. An employer will need to bear in mind the data protection principles set out in the GDPR, all of which are likely to be relevant to monitoring employees, analysing and potentially acting on the results. In broad terms, this will mean that an employer will need to ensure that:

- it is transparent and unambiguous about what monitoring is carried out and the reasons for it;
- monitoring is carried out for a specific, legitimate and identifiable reason and no other;
- no more information is gathered for the specified purpose than is necessary; and
- policies and systems are in place regarding retention and security of the information gathered through monitoring.

Before starting any large-scale monitoring exercise, it is likely that the employer will need to carry out (and document) a data protection impact assessment. This must be undertaken for processing that is likely to result in a high risk to the rights and freedoms of individuals, particularly in the case of new technologies. There are also significant limitations around the use of automated decision making (where decisions that carry significant consequences for an individual are based on assessing data without any human input) which the employer will need to take into account. Clearly this will be highly relevant where an AI system is deployed not merely to give additional insights - which will be considered by the employer - but where the system is trusted to go further and make actual decisions which impact on a given employee.

Last year the Article 29 Working Party (an advisory body comprising representatives of all the data protection authorities across the EU working under the old Data Protection Directive) produced an [updated opinion on data processing at work](#). This updates its assessment of the appropriate balance between the legitimate interests of employers against the reasonable privacy expectations of employees given the significant technological developments since its 2002 opinion on the same issue. We believe that this older opinion nevertheless provides useful guidance for the application of the technologies under the GDPR.

Helpfully the opinion covers various workplace monitoring scenarios looking at the risks that today's technologies present to employee privacy as well as the proportionality considerations including in relation to ICT usage both in and outside the workplace, time and attendance, vehicle use and wearable technology. These are helpful reading for employers wanting to get an understanding of the standards expected by the various regulatory bodies in protecting employee privacy.

The scenario on monitoring home and remote working, for example, acknowledges that this type of working presents an increased risk of unauthorised access to confidential information or a personal data breach which an employer would need to consider and address. The use, however, of all-encompassing monitoring software that logs keystrokes and mouse movements, enables webcams and logs applications used would likely be an excessive approach to mitigating this risk. Broadly, where technical methods can be used to prevent misuse or unauthorised access occurring in the first place, these should be deployed in preference to using widespread monitoring to detect it after the event.

So this means...



AI will transform the workplace bringing many benefits for not only an employer, but also its workforce. However, to ensure overall justification for its use in the context of monitoring an employer will need to identify, consider and communicate specifically:

- what monitoring it intends to carry out;
- what it will do with the results;
- the benefits and drawbacks for the business and the employees; and
- the security around the information obtained.

Contacts



Finlay McKay

Partner, Employment

T +44 131 200 7632

E finlay.mckay@cms-cmno.com



Catriona Moffatt

Professional Support Lawyer

T +44 20 7071 7340

E catriona.moffatt@cms-cmno.com