WERKSMANS
ATTORNEYS

EMPLOYMENT

Machine managers: AI monitoring in the South African workplace

15 November 2024 *5 min read*

The impact of AI on the workplace is a rapidly evolving field of study, and South Africa can look to other countries, where cutting edge AI technologies are already being utilised to enhance, improve and monitor employee performance and productivity. How these other countries are responding to these developments can be instructive for South African employers. In this regard, it is noteworthy that the U.S. Consumer Financial Protection Bureau (CFPB) is intensifying efforts to regulate workplace surveillance against growing employee concerns of privacy infringement. The CFPB has observed companies using third-party monitoring tools to assess performance and collecting biometric and personal data without transparent consent. The CFPB's oversight of this area in terms of the U.S Fair Credit Reporting Act (FCRA) grants workers the right to know and contest any data which is collected which relates to them. By applying the FCRA, the CFPB has exercised its jurisdiction over monitoring technology to prevent unfair profiling and misuse.

In partnership with the U.S Department of Labor (DOL), the CFPB's guidelines advocate that both employees and contractors must be:

1. informed of tracking practices,
2. given the chance to dispute inaccuracies,
3. be assured of data deletion [when necessary].

The concern about AI-driven surveillance risks, such as "black box" algorithms scoring employees on effectiveness and productivity, is the unintended consequence of hindering work environments by creating stress and anxiety which creates dangerous work environments. Such tools can collect sensitive information, including stress levels, body temperature and location data. US Healthcare and retail sectors have raised specific concerns that AI monitoring can detract from the quality of patient care or create high-pressure environments. A further concern is that organisations rarely provide employees clear information on how data which may be collected influences performance assessments, leading to job insecurity.

Despite these issues, the CFPB and DOL have emphasised that protecting employees' privacy rights does not conflict with technological innovation. Instead, the aim is to establish ethical standards for monitoring, ensuring that modern tech developments don't erode existing employee protections. The National Employment Law Project (a US based nonprofit advocacy organization dedicated to strengthening workers' rights) and other labour organisations have expressed that transparency around data usage, deletion protocols, and error correction are essential to prevent workplace technology from infringing on worker rights.

Overall, the CFPB's guidance signals a critical step towards reining in unchecked surveillance, balancing organizational oversight with essential privacy and labour law protections which allow US employees to limit potentially unfair or excessive monitoring practices by their employer.

In SA, the CFPB's intervention into employee monitoring in the U.S is particularly relevant under the Protection of Personal Information Act (POPIA), – which enshrines the right to privacy, mandating that any collection, use, or processing of personal data. Employers using AI-driven surveillance and monitoring tools in South Africa would need to justify their monitoring practices under POPIA's principles of transparency, data minimality, and lawfulness, ensuring only necessary data is collected

and used for legitimate purposes. In addition, employers would need to ensure that any such monitoring is carried out with the required express consent of the employee, as contemplated in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, or at least that such monitoring of employee communications is lawful under the provisions of RICA which allow an employer to do so in respect of communications by employees which are made in the course of carrying on the business of the employer.

In any circumstances, care needs to be taken to manage use of AI tools which perform these monitoring functions, especially where they are used for profiling, automated decision making about the employee (e.g. for performance management, salary increases and incentives, promotions etc.) and/or to collect and analyse biometric information or other sensitive information. Caution is also advised where the lines blur between information collected in relation to employee work activities and productivity and accessing employee health information (e.g. stress levels, vitals) and information relating to their personal life (e.g. information of employees' home environments or family/personal matters where work from home activities are tracked).

Additionally, employees must have the right to know what data is collected, how it is being processed, and to challenge inaccuracies or overreach, similar to the Fair Credit Reporting Act in the U.S.

POPIA reinforces the principle that employers should avoid excessively intrusive monitoring that could violate personal privacy, particularly where technologies track sensitive information. In line with the spirit of POPIA, employers in South Africa should ensure that employee surveillance does not foster a coercive or mistrustful environment, emphasizing a balanced approach where employee rights to privacy coexist with the legitimate interests of workplace management. As technologies evolve, the principles of POPIA remind South African employers of the imperative to uphold privacy in the workplace, even as they seek to incorporate performance-monitoring tools.



Preeta Bhagattjee

Head of Technology & Innovation

View Profile



Bradley Workman-Davies

Director

View Profile