The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

WATCHING THE WORKER : HOW WORKPLACE SURVEILLANCE AND ALGORITHMIC MANAGEMENT UNDERMINE PRODUCTIVITY AND EMPLOYEE PRIVACY

~ Subiksha Merin

INTRODUCTION

The contemporary workplace is increasingly governed by data. Employers across sectors deploy digital surveillance tools and algorithmic management systems in the pursuit of efficiency, productivity, and managerial control. From keystroke monitoring and biometric attendance systems to AI-driven performance scoring and predictive analytics, employees are subjected to continuous and granular observation. These practices are routinely justified as productivity-enhancing measures - neutral, objective, and technologically superior alternatives to human supervision.

However, this assumption rests on a flawed understanding of both human productivity and technological objectivity. Empirical evidence and emerging legal scholarship suggest that excessive workplace surveillance often undermines productivity, distorts performance evaluation, and erodes trust, while fully automated algorithmic management systems - particularly those operating without human oversight - prove to be inaccurate, biased, and incompatible with principles of fairness and dignity. This article argues that surveillance-driven productivity regimes are counterproductive and that meaningful human oversight is indispensable for fostering productive, equitable, and lawful workplaces.

Drawing comparative insights from the European Union's Artificial Intelligence Act (EU AI Act), the article demonstrates how contemporary regulatory approaches increasingly recognize the risks posed by automated decision-making in employment and mandate safeguards that remain largely absent in jurisdictions such as India.

THE RISE OF WORKPLACE SURVEILLANCE AND DATAFIED LABOUR

Workplace surveillance has undergone a qualitative transformation. Traditional supervision- episodic, visible, and contextual - has been replaced by continuous, invisible, and automated monitoring. Digital technologies enable employers to collect vast quantities of data relating to employee behaviour, communication, productivity, location, biometrics, and even emotional states.

This shift has resulted in the datafication of labour, where employees are reduced to streams of quantifiable signals. Surveillance no longer merely observes work; it constructs narratives of performance, often detached from the lived realities of human labour. Crucially, data collected is rarely static. Primary data is routinely repurposed as a data feed to generate secondary and inferential data, allowing employers to predict behaviour, assess "risk", and categorise workers.

In this environment, the boundaries between monitoring, management, and control collapse. Surveillance becomes a tool not only of observation, but of behavioural modification and discipline.

EMPLOYEE SURVEILLANCE

The modern workplace has become one of the most intensive sites of personal data extraction. Employers increasingly deploy digital surveillance technologies that track not only how employees work, but how they behave, communicate, move, and even feel. While such practices are often justified as necessary for efficiency, security, or productivity, they raise profound concerns about the systematic invasion of employee privacy.

Unlike consumers or citizens in public spaces, employees are subjected to surveillance in a context marked by economic dependency and unequal bargaining power. The workplace thus presents a unique privacy challenge: surveillance here is neither voluntary nor avoidable, and the consequences of resistance can directly affect livelihood. This article argues that contemporary workplace surveillance constitutes a serious invasion of employee privacy, one that existing legal frameworks - particularly in India - are ill-equipped to address.

Employee privacy is often misunderstood as a narrow right to secrecy or confidentiality. In reality, privacy in the employment context encompasses autonomy, dignity, and control over personal information. As recognised in constitutional jurisprudence, particularly in *Justice K.S.*

Puttaswamy v. Union of India, privacy includes informational self-determination- the ability to control how one's personal data is collected, processed, and used.

In the workplace, this interest is especially vulnerable. Employees are required to disclose personal information as a condition of employment and are subjected to monitoring that extends well beyond the performance of assigned tasks. Privacy violations thus occur not merely when data is disclosed externally, but when continuous observation strips individuals of decisional and informational autonomy.

Crucially, surveillance is no longer limited to the workplace premises or working hours. Remote work technologies enable monitoring within employees' homes, blurring the boundary between professional and private life. Data collected is often retained indefinitely, aggregated across platforms, and repurposed for uses far removed from its original collection purpose.

This constant monitoring transforms employees into objects of data extraction, where privacy is compromised not by a single intrusive act, but by pervasive and cumulative observation.

One of the gravest privacy risks in the workplace arises from the ability of surveillance systems to infer sensitive personal attributes. Such inferences, even when probabilistic, have material consequences. Employees perceived as having higher health risks or caregiving responsibilities are often treated as economic liabilities. They may be excluded from promotions, denied leadership roles, or subtly sidelined in performance evaluations.

THE PRODUCTIVITY MYTH: HOW SURVEILLANCE UNDERMINES PERFORMANCE

The central justification for workplace surveillance is productivity enhancement. Yet this logic is deeply flawed.

First, constant monitoring generates stress, anxiety, and cognitive overload, which directly impair performance. Employees subjected to surveillance are incentivized to optimize for metrics rather than outcomes, engaging in performative compliance-appearing busy, maximizing screen time, or prioritizing speed over quality. This phenomenon leads to shallow productivity gains at best and long-term inefficiencies at worst.

Second, surveillance corrodes trust, a cornerstone of productive organisations. Trust-based environments foster autonomy, creativity, collaboration, and innovation. Surveillance replaces trust with suspicion, signaling that employees are inherently untrustworthy. This results in disengagement, reduced morale, and increased attrition-outcomes fundamentally at odds with productivity objectives.

Third, surveillance tools are structurally biased towards quantifiable labour, marginalising forms of work that are essential but difficult to measure, such as mentoring, emotional labour, teamwork, and problem-solving. Employees are penalised for engaging in socially valuable but non-measurable activities, distorting incentives and degrading workplace culture. Surveillance-driven productivity regimes reflect a misalignment between what is measured and what truly constitutes productive work.

ALGORITHMIC MANAGEMENT AND THE ILLUSION OF OBJECTIVITY

Algorithmic management represents the most advanced manifestation of workplace surveillance. In such systems, algorithms determine work allocation, evaluate performance, trigger disciplinary action, and even effect termination. Employers often portray these systems as objective and neutral, claiming that automation eliminates human bias.

In reality, algorithmic systems are neither neutral nor accurate assessors of human productivity. Algorithms rely on historical data and simplified proxies that fail to capture context, nuance, or legitimate variability in human performance. They cannot account for illness, caregiving responsibilities, collaborative work patterns, or structural inequalities that shape labour outcomes.

Further, algorithmic systems often embed and amplify existing biases. Performance metrics such as availability, response time, or customer ratings disproportionately disadvantage certain groups, including persons with disabilities, pregnant workers, caregivers, and older employees. Because these systems operate opaquely, affected workers are rarely able to identify the basis of adverse decisions, let alone challenge them.

When productivity assessment is fully automated and devoid of human oversight, procedural fairness collapses. Decisions affecting livelihood are rendered inscrutable, unchallengeable, and unaccountable.

LESSONS FROM THE EU AI ACT: EMPLOYMENT AS A HIGH-RISK DOMAIN

The EU AI Act offers a critical comparative lens through which to evaluate workplace surveillance and algorithmic management. Notably, the Act classifies AI systems used in employment, worker management, and access to self-employment as "high-risk AI systems". This classification is premised on the recognition that automated decision-making in employment contexts has profound implications for fundamental rights, including privacy, equality, and dignity.

Under the EU AI Act, high-risk AI systems are subject to stringent obligations, including:

- Risk assessment and mitigation to prevent discriminatory outcomes,
- High-quality, representative datasets to reduce bias,
- Transparency obligations, ensuring users understand system capabilities and limitations,
- Human oversight requirements, mandating that AI systems do not operate autonomously where rights and livelihoods are at stake.

Crucially, the Act rejects the notion that efficiency alone can justify automation in employment. Instead, it insists that human agency and accountability must remain central.

HUMAN OVERSIGHT AS A LEGAL AND PRODUCTIVITY IMPERATIVE

The EU AI Act's insistence on human oversight reflects a broader recognition that automation must remain subordinate to human judgment. In employment contexts, human oversight serves multiple functions.

First, it ensures contextual decision-making, allowing managers to interpret data in light of individual circumstances. Second, it introduces accountability, as human decision-makers can be questioned, challenged, and held responsible. Third, it mitigates bias by enabling correction of algorithmic errors and discriminatory outcomes.

From a productivity perspective, human oversight enhances trust, legitimacy, and employee engagement. Workers are more likely to accept adverse decisions when they are reasoned, transparent, and subject to review. Thus, oversight is not an obstacle to efficiency; it is a prerequisite for sustainable productivity.

SURVEILLANCE, BIAS, AND DISCRIMINATION

The combination of surveillance and algorithmic management poses acute risks of covert discrimination. Data collected for ostensibly neutral purposes can be used to infer sensitive attributes such as disability, health status, pregnancy, or reproductive intent. Such inferences often result in exclusion from promotions, reduced work opportunities, or termination.

The opacity of algorithmic systems makes such discrimination exceptionally difficult to detect or prove, effectively insulating employers from accountability. This undermines labour protections and equality guarantees, rendering them illusory in data-driven workplaces.

CONCLUSION: REIMAGINING PRODUCTIVITY IN DATA-DRIVEN WORKPLACES

Employee privacy is not an obstacle to effective management; it is a precondition for dignified and sustainable work. Workplace surveillance that treats employees as perpetual data subjects undermines autonomy, erodes trust, and facilitates discrimination. As work becomes increasingly mediated by data and algorithms, the law must confront the reality that privacy violations in the workplace are systemic rather than exceptional. Protecting employee privacy requires moving beyond formal consent and towards structural safeguards, transparency, and accountability.

Without such intervention, the workplace risks becoming a zone where privacy is permanently suspended-where individuals must trade dignity for employment. A legal order committed to constitutional values cannot allow such a trade-off to become the norm.

Workplace surveillance and fully automated algorithmic management are premised on a reductive vision of productivity - one that equates constant visibility with efficiency and automation with objectivity. This article has demonstrated that such assumptions are empirically and normatively unsound. Drawing from the EU AI Act, it is evident that employment is a domain where automation demands heightened scrutiny, not blind adoption. Productivity cannot be engineered through surveillance alone; it emerges from trust, autonomy, fairness, and meaningful human engagement. Human oversight is not merely a safeguard—it is central to both dignity and productivity.

Legal frameworks must ensure that technology serves human labour, rather than subordinating it. Without such recalibration, the pursuit of efficiency risks eroding not only privacy and equality, but the very foundations of productive work.