WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Workplace Surveillance and Employee Data Governance in India: Re-reading the Digital Personal Data Protection Framework Through the Lens of White-Collar Employment

Mangalam D. Joshi[a], Dr. Satnam Tuteja[b]

[a]Research Scholar, Law, Swaminarayan University, Kalol, Gandhinagar, Gujarat, India
[b]Dean, Law, Swaminarayan University, Kalol, Gandhinagar, Gujarat, India

A B S T R A C T :

Digital monitoring has become an ordinary feature of white-collar employment: employers may log device activity, inspect work communications, use productivity analytics, deploy biometric access systems, or evaluate workers through algorithmic tools. These practices raise a problem that is not resolved simply by asking whether an employer has a legitimate business purpose. The legal question is how to reconcile workplace security and organisational accountability with the employee's privacy, autonomy, dignity and ability to challenge consequential decisions. This doctrinal paper examines that question at the intersection of India's Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, 2025, constitutional privacy principles and the four Labour Codes brought into force in November 2025. Its central contribution is a temporal and functional analysis: the DPDP Act's employment-related legitimate-use provision is not fully operative immediately, because the commencement notification stages the substantive provisions over eighteen months from November 2025. The paper therefore distinguishes the law currently operative from the framework scheduled to commence later, rather than treating the Act as already fully enforceable. It argues that a general data-protection framework, even when operational, does not by itself supply workplace-specific standards for necessity, proportionality, notice, retention, human review and contestability. The paper proposes a model of employment data governance built around purpose limitation, graduated monitoring, impact assessment for high-risk tools, access controls, short retention periods, worker-facing explanations and independent grievance review. It concludes that India should develop an employment-specific code or binding rules that complement, rather than duplicate, data-protection law and labour regulation.

Keywords: white-collar employees; workplace surveillance; employee privacy; Digital Personal Data Protection Act, 2023; algorithmic management; Labour Codes; data governance

Introduction

White-collar work increasingly leaves a digital trace. Email and collaboration platforms record communication metadata; virtual private networks and endpoint tools record access; attendance systems collect location or biometric information; and productivity software can translate keystrokes, screen activity, task completion and response times into performance indicators. Employers may reasonably need some of this information to protect confidential data, investigate security incidents, administer benefits and coordinate distributed teams. Yet the same systems can make continuous observation technically possible, including when the employee is working from home or outside conventional office hours.

The legal difficulty is not captured by a simple opposition between privacy and business efficiency. Workplace data may be collected for one stated purpose and later reused for performance scoring, discipline, promotion or termination. Data that appears innocuous in isolation can reveal patterns of health, family responsibilities, religious practice, union activity or working habits when aggregated. Automated inferences may also be inaccurate, difficult to explain and hard for an employee to contest because the underlying system is proprietary. The power imbalance of employment complicates any claim that the worker has freely agreed to monitoring.

This paper examines workplace surveillance through a narrow question: what legal standards should govern an employer's collection, analysis, retention and use of personal data about white-collar employees in India? The paper does not repeat a general evaluation of the legal protection of white-collar employees or a broad account of the Labour Codes. Instead, it studies the intersection between employment power and personal-data governance, with particular attention to the staged commencement of the DPDP Act. The argument is that legal authorisation to process data for employment-related purposes should not be mistaken for an unlimited permission to monitor.

The paper proceeds in six parts. After stating its method and identifying the legal baseline, it analyses the relationship between employment-related processing and employee consent, identifies regulatory gaps, and develops a proposed governance model. It concludes with recommendations directed to legislators, regulators and employers.

Research Methodology and Scope

This study adopts a doctrinal and analytical methodology. Primary sources include the Constitution of India, the DPDP Act, 2023, the DPDP Rules, 2025, the commencement notification issued under the Act, relevant Labour Codes and Supreme Court authority on privacy. Secondary materials are used to situate workplace monitoring within contemporary data-governance debates. No interviews, surveys or other empirical data collection are claimed. Accordingly, the paper makes normative legal arguments rather than empirical claims about the prevalence or effects of surveillance in Indian workplaces.

The scope is limited to employees in conventional white-collar employment, including professional, administrative, technical and managerial roles. It does not assume that every person described as a white-collar employee falls within every labour-law definition. Nor does it treat platform workers and independent contractors as automatically equivalent to employees. Those classifications depend on the applicable statute and the actual relationship. The focus here is the personal data generated by an employment relationship, regardless of whether a particular employee is classified as a "worker" for a specific labour-law remedy.

A temporal distinction is essential. The Government notified the DPDP Rules in November 2025 and issued a phased commencement notification for the Act. Several institutional and rule-making provisions commenced on publication, while many substantive processing duties and data-principal rights—including section 7's legitimate-use provision—were scheduled to commence eighteen months after 13 November 2025. This paper therefore does not represent all substantive DPDP provisions as fully operative on the date of writing. The recommendations are designed for the transition period and the expected operation of the full framework.

The Legal Architecture: Privacy, Data Protection and Employment

1.1. Constitutional privacy as a constraint on workplace power

In Justice K.S. Puttaswamy (Retd.) v Union of India, the Supreme Court recognised privacy as a fundamental right protected by Article 21 and connected constitutional freedoms (Supreme Court of India, 2017). The decision is not a workplace-surveillance code, and its application to every private-employer monitoring practice cannot be assumed without doctrinal analysis. Nevertheless, its emphasis on legality, legitimate purpose and proportionality provides a constitutional vocabulary for assessing state action and for informing the development of privacy-sensitive legal standards. The central insight is that a legitimate objective does not automatically validate every means used to achieve it.

For workplace governance, proportionality can be operationalised through four questions: is the monitoring authorised by law or a valid legal basis; does it pursue a specific legitimate purpose; is the data collection rationally connected to that purpose and no more intrusive than reasonably necessary; and are safeguards available against arbitrary use? An employer investigating a targeted data leak presents a different case from an employer recording every keystroke of every employee indefinitely. Treating these cases alike would erase the distinction between a justified security measure and generalised surveillance.

1.2. The DPDP Act and the employment-related legitimate-use provision

The Digital Personal Data Protection Act, 2023 creates a framework for processing digital personal data and defines roles such as Data Principal and Data Fiduciary (Government of India, 2023). Section 7 identifies certain legitimate uses for which personal data may be processed. Clause (i) refers to purposes of employment and purposes related to safeguarding an employer from loss or liability, including prevention of corporate espionage, protection of trade secrets and intellectual property, and provision of a service or benefit sought by an employee. The provision is important because employment processing may not always be realistically based on freely given consent.

However, three qualifications matter. First, the statutory text is purpose-linked: employment-related processing is not the same as unrestricted collection for any purpose an employer later finds useful. Secondly, the provision must be read with the Act as a whole, its applicable duties, rules and commencement schedule. Thirdly, the existence of a legitimate-use ground does not answer all workplace questions: it does not itself prescribe a universal monitoring notice, maximum retention period, mandatory human review of algorithmic scores, or a sector-neutral procedure for challenging surveillance-derived discipline.

The commencement notification makes timing especially significant. The DPDP Act's substantive provisions, including sections 3 to 17 and section 7, are scheduled to come into force eighteen months after publication of the notification dated 13 November 2025. Therefore, as at October 2026, the full set of substantive obligations and employee-facing rights should not be described as already operative merely because the Act and Rules have been notified. Employers and researchers must distinguish enacted law, provisions already commenced, and provisions awaiting commencement. This temporal precision is particularly important when discussing an employee's current legal remedies.

1.3. The Labour Codes and the missing workplace-data layer

The four Labour Codes—on wages, industrial relations, social security, and occupational safety, health and working conditions—were brought into force from 21 November 2025 according to the Ministry of Labour and Employment (Ministry of Labour and Employment, 2025). They consolidate important parts of employment regulation, but they do not create a comprehensive, employment-specific regime for digital monitoring. Their definitions and protections continue to operate according to their respective statutory purposes; they should not be assumed to resolve questions about algorithmic profiling, workplace telemetry or data reuse simply because the codes modernise labour regulation.

The DPDP framework and the Labour Codes are therefore complementary but not interchangeable. Data-protection law addresses processing of digital personal data, while labour legislation regulates matters such as wages, industrial relations, social security and occupational conditions. Neither framework, taken alone, gives a complete answer to whether a productivity score generated by continuous monitoring can fairly support a disciplinary decision, how an employee should challenge an inaccurate inference, or what level of monitoring is proportionate for ordinary performance management. This is the specific regulatory gap addressed by the paper.

Employment Data and the Limits of Consent

1.4. Why consent is structurally fragile in employment

Consent is often presented as the natural solution to workplace data collection: an employee receives a policy, clicks "accept", or signs a clause in the employment contract. Yet the employment relationship is characterised by unequal bargaining power and dependency on wages, benefits and career progression. A refusal may be formally possible but practically costly. In many workplaces, the employee cannot negotiate whether the organisation will use access logs, endpoint security software or productivity platforms.

The statutory recognition of employment-related legitimate use reflects this practical problem, but it should not be interpreted as a reason to abandon employee agency. Instead, the legal model should distinguish between processing necessary for the employment relationship or a demonstrable security purpose and optional or intrusive monitoring. Core processing may rest on an applicable statutory basis, while optional monitoring should require a separate, meaningful choice where feasible. A single blanket consent clause should not validate every future category of data collection or secondary use.

1.5. Purpose drift and secondary use

Purpose drift occurs when information collected for one reason is repurposed for another. A login record collected to secure a network may later be used to infer that an employee is insufficiently committed; a camera system introduced for physical safety may become a tool for measuring time at a desk; or a meeting-transcription service may generate behavioural analytics not contemplated when employees began using it. These uses differ in impact and cannot be justified merely by pointing to the original collection.

A workable rule should require employers to define each purpose at the level of meaningful specificity. "Business purposes" is too broad to tell an employee whether data will be used for cybersecurity, attendance, productivity ranking or disciplinary proceedings. Material changes should trigger renewed notice and a documented assessment of necessity. Data collected for security should not be silently converted into a general performance dataset unless the additional use is independently justified, lawful and proportionate.

1.6. Inference, accuracy and contestability

Modern monitoring systems can transform behavioural traces into inferences about productivity, risk or engagement. Such inferences are not direct observations of the employee's contribution. Keyboard activity may fail to capture reading, mentoring, planning or complex reasoning; a long period without screen activity may reflect a telephone call, a paper document or a reasonable accommodation. A score may also encode assumptions about working style that disadvantage employees with disabilities, caregiving responsibilities or different communication practices.

Procedural fairness therefore requires more than access to raw data. Where a consequential employment decision relies materially on a surveillance-derived score or automated recommendation, the employee should receive a comprehensible explanation of the relevant factors, a chance to correct factual errors, and access to meaningful human review. The reviewer should have authority to change the outcome rather than merely confirm the system's recommendation. These safeguards are proposed as workplace standards; they should not be misrepresented as already expressly guaranteed in identical form by the DPDP Act.

A Proposed Employment Data Governance Model

1.7. A graduated approach to monitoring

Monitoring should be classified according to purpose, intrusiveness and likely consequence. Routine security logging, such as recording access to protected systems, may be justified by a clear security need and limited retention. Targeted investigation of a credible incident may justify more intrusive collection, subject to documented authorisation and a narrow scope. Continuous screen recording, webcam monitoring, keystroke capture or emotion inference should be treated as high-risk practices requiring exceptional justification, not as default management tools.

A graduated approach avoids the false choice between banning all monitoring and permitting everything disclosed in a policy. It recognises that an organisation may need stronger controls for highly sensitive information while imposing stricter conditions on tools that observe personal behaviour or infer psychological states. The more intrusive the tool and the greater the employment consequences, the stronger the required justification and safeguards should be.

1.8. Notice and a monitoring register

Every employer using systematic digital monitoring should maintain an accessible monitoring register. For each tool, the register should identify: the data categories collected; the specific purpose; the legal basis relied upon; the persons or vendors with access; retention and deletion periods; whether data informs performance or disciplinary decisions; and the contact point for questions or complaints. Employees should receive a concise notice in plain language before monitoring begins and when a material change occurs.

Notice should be practical rather than ceremonial. A dense policy hidden in an intranet does not provide meaningful understanding. The employee should be able to determine whether the employer records message content or only metadata, whether a productivity score is generated, whether data is transferred to a vendor, and how long records are retained. The register also creates an internal audit trail for regulators, employee representatives and courts.

1.9. Necessity, proportionality and data minimisation

Before introducing a high-risk monitoring tool, the employer should document the problem it seeks to solve, the evidence that the problem exists, the less intrusive alternatives considered, and why those alternatives are insufficient. The assessment should examine false positives, unequal effects across job roles, possible chilling effects on legitimate activity and the consequences of misuse. Monitoring should be limited by role, time, system or incident where possible.

Data minimisation should apply throughout the lifecycle. If a security objective can be achieved through access logs, continuous video capture should not be the default. If aggregate workload metrics are sufficient, individual-level behavioural scoring may be unnecessary. If raw data is needed only briefly to investigate an incident, it should not be retained indefinitely for possible future use. A short retention schedule should be the norm, with documented exceptions for litigation holds or legal obligations.

1.10. Human review and fair process

Where surveillance information may lead to warning, loss of bonus, demotion or termination, an employee should be informed of the substance of the concern and given a reasonable opportunity to respond. The employer should disclose the material relied upon to the extent consistent with legitimate security and third-party privacy interests. Any redaction should be reasoned rather than used to conceal the basis of the decision.

Automated systems should not be the final decision-maker in serious employment matters. Human review must be informed, independent enough to challenge the tool, and supported by records of the reasoning adopted. The decision-maker should consider contextual explanations and should not treat a numerical score as conclusive proof of misconduct or poor performance. These requirements connect data governance with procedural fairness without assuming that every private employment dispute is automatically governed by constitutional due process.

1.11. Grievance, audit and vendor accountability

Employees need a clear route to question monitoring, request correction of inaccurate data, challenge inappropriate secondary use and complain about disproportionate practices. An internal grievance channel should have a defined response period and should not be controlled solely by the manager whose decision is challenged. High-risk systems should be periodically audited for accuracy, access controls, retention compliance and disparate effects.

Employers remain responsible for selecting and supervising technology vendors. Contracts with vendors should define permitted processing, confidentiality, security, deletion, incident reporting, access by subcontractors and restrictions on using employee data to train unrelated models. A vendor's claim that its algorithm is proprietary should not eliminate the employer's ability to explain how employee data affects consequential decisions. Where the employer cannot obtain sufficient information to assess a tool's risks, that limitation weighs against using it for high-stakes employment decisions.

Comparative and Normative Lessons

Comparative law offers useful design principles, but legal transplants must be careful. The European Union's General Data Protection Regulation, including its principles of purpose limitation, data minimisation, transparency and accountability, illustrates how general data-protection norms can discipline organisational processing. The EU's regulatory debate on high-risk artificial intelligence also highlights the importance of risk classification and human oversight where automated systems affect employment. These instruments do not apply as Indian law merely because they offer persuasive models.

The relevant lesson is institutional rather than mechanical: employment data governance should combine a general privacy framework with rules sensitive to the special power imbalance and consequences of employment decisions. A workplace-specific instrument could define high-risk monitoring, require impact assessments for specified tools, set minimum notice standards and establish a procedure for contesting decisions. It should also provide exceptions for genuine security investigations, but subject those exceptions to documentation, access controls and review.

An Indian model should avoid treating every digital record as inherently abusive. Cybersecurity logs, access-control records and fraud investigations can protect employees as well as employers. The normative test is whether the measure is necessary and proportionate to a defined purpose, whether less intrusive alternatives were considered, and whether the resulting data is used fairly. The focus should be on accountable monitoring rather than an absolute prohibition.

Findings and Recommendations

The analysis yields five principal findings. First, workplace surveillance is not merely a privacy issue: it can influence wages, appraisal, discipline, promotion and job continuity. Secondly, the employment-related legitimate-use ground in section 7 of the DPDP Act is purpose-specific and must be read in the context of the Act's commencement schedule. Thirdly, the Labour Codes do not supply a complete set of workplace-specific standards for digital monitoring. Fourthly, consent alone is an unreliable safeguard where employees cannot realistically refuse. Fifthly, procedural protections are necessary where data-derived inferences affect employment outcomes.

Accordingly, the paper recommends that the Central Government, in consultation with labour and data-protection authorities, develop binding employment data-governance rules. These should require: (i) clear, role-specific monitoring notices; (ii) a documented necessity and proportionality assessment for high-risk tools; (iii) a prohibition on indiscriminate or covert continuous monitoring except under narrowly defined and reviewable circumstances; (iv) purpose limitation and retention schedules; (v) access and correction mechanisms; (vi) meaningful human review of consequential decisions; (vii) periodic audits and vendor accountability; and (viii) a grievance mechanism protected against retaliation.

Employers should implement these standards before the full substantive DPDP framework commences, rather than waiting for the final statutory deadline. The transition period provides an opportunity to map data flows, revise employment policies, review vendor contracts, delete unnecessary records and train HR, IT and compliance teams. Regulators should issue sector-sensitive guidance that recognises differences between a bank handling highly confidential information, a software firm protecting source code and an ordinary office using basic attendance systems.

Conclusion

The rise of workplace surveillance exposes a gap between the technical capacity to monitor and the legal standards that should govern monitoring. The DPDP Act offers an important framework for personal-data processing, and section 7 expressly recognises employment-related legitimate use. But neither a legitimate purpose nor a broad policy notice should be treated as a blank cheque for continuous observation, opaque scoring or unrestricted secondary use. The staged commencement of the DPDP Act also makes it essential to distinguish provisions already in force from substantive duties and rights scheduled to commence later.

The central proposal of this paper is an employment-specific data-governance layer built around necessity, proportionality, transparency, minimisation, contestability and accountable human review. Such a framework would protect legitimate security and business interests while reducing the risk that digital tools silently convert ordinary employment into continuous behavioural assessment. Its contribution is to move the debate beyond whether employers may monitor and toward the more precise legal question: under what conditions, for which purposes, with what limits and subject to what remedies may employee data be used?

REFERENCES

- Constitution of India.
- Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
- Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
- Ministry of Electronics and Information Technology. (2025, November 13). Notification G.S.R. 843(E): Enforcement timeline for the Digital Personal Data Protection Act, 2023. Gazette of India, Extraordinary.
- Ministry of Labour and Employment. (2025, November 21). Government makes the four Labour Codes effective to simplify and streamline labour laws. Press Information Bureau, Government of India.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
- Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.