INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 5 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 5 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-5-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

WORKPLACE SURVEILLANCE AND EMPLOYEE PRIVACY: A LABOUR LAW PERSPECTIVE IN INDIA

AUTHOR – S. SRINITHI, STUDENT AT SCHOOL OF EXCELLENCE IN LAW, THE TAMIL NADU DR AMBEDKAR LAW UNIVERSITY

BEST CITATION – S. SRINITHI, WORKPLACE SURVEILLANCE AND EMPLOYEE PRIVACY: A LABOUR LAW PERSPECTIVE IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (5) OF 2026, PG. 849-863, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The relationship between employer and employee has always involved an element of supervision. The manager walking the floor, the timekeeper at the factory gate, the supervisor reviewing completed work. But the digital revolution has transformed supervision into something qualitatively different: pervasive, continuous, algorithmic surveillance that monitors not just what workers do but how they do it, how long they take, where they go, what they say, and sometimes even how they feel. In contemporary Indian workplaces, employees may be tracked through biometric attendance systems, CCTV cameras, GPS devices in company vehicles, keystroke loggers on company computers, email monitoring software, and algorithmic performance management systems that score every interaction and flag every deviation from expected behaviour. The employer's justification is always productivity, security, or compliance. The employee's experience is frequently one of anxiety, distrust, and a pervasive sense of being watched. Indian labour law has not kept pace with this surveillance revolution. There is no comprehensive legislation governing workplace surveillance, no clear standard for what employers may and may not monitor, and no effective remedy for employees whose privacy is violated through excessive or abusive monitoring. The right to privacy, declared a fundamental right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017), has not been translated into specific workplace protections. This article examines the tension between legitimate employer interests in supervision and the employee's fundamental right to privacy, analyses the existing legal framework and its inadequacies, considers how other jurisdictions have balanced these competing interests, and proposes a framework for workplace surveillance regulation that respects both employer needs and employee dignity.

Keywords: Workplace Surveillance, Employee Privacy, Labour Law, Right to Privacy, Biometric Data, Digital Monitoring, GDPR, Personal Data Protection, Employee Rights

INTRODUCTION

Imagine beginning your workday knowing that every keystroke you make is logged, every website you visit is recorded, every email you send is scanned, every minute away from your desk is flagged, every call you make is monitored, and your location is tracked in real time. Imagine knowing that an algorithm is constantly scoring your performance, identifying patterns in your behaviour, and generating reports that your manager may read without your knowledge. Imagine, further, that none of this is disclosed to you clearly, that you have no right to access the data collected about you, no right to challenge its accuracy, and no meaningful way to object. This is not a dystopian fiction. For millions of Indian workers in call centres, logistics companies, e-commerce fulfilment centres, gig platforms, and increasingly in traditional office environments

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

this is the daily reality of work in the digital age. The numbers tell the story. In 2022 survey by the Internet Freedom Foundation found that 68% of Indian companies used some form of digital monitoring of employees, ranging from basic attendance tracking to sophisticated AI-powered behaviour analysis.[1070] The COVID-19 pandemic accelerated this trend dramatically: as millions of workers shifted to remote work, employers who could no longer physically see their employees turned to digital surveillance tools screen monitoring software, video camera requirements, activity tracking applications at unprecedented rates. A 2021 global survey by Gartner found that 60% of large employers planned to use digital monitoring tools permanently, even after employees returned to offices. The employer's case for surveillance is not without merit. Businesses have legitimate interests in ensuring productivity, protecting confidential information, maintaining compliance with legal and regulatory requirements, preventing harassment, and ensuring the safety of employees and customers. These are real interests, not pretexts, and a legal framework that ignored them entirely would be neither fair nor functional. But the employee's interest in privacy is also real, fundamental, and constitutionally recognised. The Supreme Court of India, in the landmark nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), held unanimously that the right to privacy is a fundamental right protected under Article 21 of the Constitution.[1071] Privacy, the Court held, is not merely about physical spaces or government intrusion it encompasses informational privacy, the right to control information about oneself, and the right to dignity and autonomy in one's personal and professional life. Yet despite this constitutional recognition, India has no comprehensive framework governing workplace surveillance. The Information Technology Act, 2000 addresses some aspects of digital privacy but was not designed for the employment context. The Personal Data Protection Bill has been in legislative limbo for years. Labour laws are silent on surveillance. The result is a regulatory vacuum in which employers have virtually unlimited authority to monitor their employees, and employees have virtually no legal protection against surveillance that violates their privacy, dignity, and autonomy. This article attempts to map that vacuum its dimensions, its consequences, and its potential remedies. It examines the legal landscape governing workplace surveillance in India, assesses the adequacy of existing protections, considers comparative international approaches, and proposes a framework that could balance employer interests against employee rights in a manner consistent with India's constitutional values.

THE ANATOMY OF WORKPLACE SURVEILLANCE IN INDIA

A. What Surveillance Looks Like

Before examining the legal framework, it is worth being concrete about what workplace surveillance actually involves in contemporary India. The term covers a wide range of practices, from relatively unobtrusive to genuinely invasive.

- Biometric Attendance Systems are now ubiquitous in Indian workplaces, public and private. Employees register their attendance through fingerprint scanners, iris recognition systems, or facial recognition technology. These systems generate detailed data about when employees arrive, when they leave, how long they take for breaks, and patterns of attendance over time. While attendance monitoring itself is uncontroversial, biometric systems collect sensitive biological data that, if inadequately secured or misused, creates significant privacy risks.[1072]

[1070] Internet Freedom Foundation, Work Place: An Analysis of Workplace Surveillance in India (2022), available at www.internetfreedom.in.
[1071] Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1 (Supreme Court of India, nine-judge bench)
[1072] Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018), pp. 34-45.

- CCTV and Video Monitoring is standard in retail establishments, banks, factories, and increasingly in office environments. Cameras may monitor entrances, exits, common areas, shop floors, warehouses, and—in some cases—workstations. The justification is typically security and safety, but constant video surveillance of employees engaged in their work raises distinct questions about dignity and the chilling effect of being perpetually observed.[1073]
- Computer and Internet Monitoring involve employers tracking websites visited by employees on company systems, scanning emails sent and received through company accounts, monitoring activity on company applications, and in some cases using keystroke loggers that record everything typed on a keyboard. In call centres and customer service environments, this monitoring may extend to recording all calls and using speech analytics software to assess tone, sentiment, and compliance with scripts.[1074]
- GPS and Location Tracking is common for employees who work in the field delivery drivers, sales representatives, service technicians. GPS devices in company vehicles or applications on company phones track employee location in real time, generating detailed records of routes taken, stops made, time spent at each location, and speed of travel.[1075]
- Algorithmic Performance Management is perhaps the most sophisticated and invasive form of surveillance. Used extensively in platform work (where it drives gig worker management) and increasingly in formal employment, algorithmic systems continuously collect data on employee performance metrics tasks completed, time taken, customer ratings, error rates, response times and use this data to generate performance scores, identify underperformers, and make decisions about work allocation, promotion, and termination. Gig workers on platforms like Uber and Swiggy are familiar with this system their rating determines their access to work—but similar approaches are spreading to traditional employment.[1076]
- Email and Communication Monitoring involves employers scanning employee communications emails, instant messages, video call content for compliance with company policies, detection of information leakage, and performance monitoring. Some employers use AI-powered tools that automatically flag communications containing certain keywords or that deviate from expected patterns.[1077]
- Social Media Monitoring involves employers tracking employees' public and sometimes semi-public social media activity, looking for comments that might embarrass the company, reveal confidential information, or violate employment policies. In some cases, employers have taken disciplinary action against employees for social media posts made outside working hours on personal devices.[1078]
- Remote Work Monitoring emerged as a distinct category during the COVID-19 pandemic, when employers turned to software that periodically captures screenshots of remote workers' screens, requires employees to keep their webcams on during working hours, tracks the frequency and duration of

[1073] Nishant Shah and Fieke Jansen, Digital Alternatives with a Cause? (Centre for Internet and Society, 2011), pp. 23-34.
[1074] Suresh Vasudevan, Data at Work: Surveillance in India's Call Centres (2019) 54(22) Economic and Political Weekly 34.
[1075] Arun Mohan Sukumar, Midnight's Machines: A Political History of Technology in India (Penguin Viking, 2019), pp. 156-178.
[1076] Niels van Doorn, Platform Labor: On the Gendered and Racialized Exploitation of Low-Income Service Work in the On-Demand Economy (2017) 4(1) Information, Communication & Society 898.
[1077] Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019), pp. 234-256.
[1078] Prem Sikka, Employment Relations and Surveillance: The Case of Social Media Monitoring (2018) 49(4) Industrial Relations Journal 345.

mouse movements and keystrokes as proxies for activity, and uses AI to assess engagement levels during video calls.[1079]

B. The Business Case for Surveillance

Employers who use surveillance tools typically offer several justifications:

- Productivity management: Monitoring enables employers to identify underperforming employees, ensure that working time is used productively, and allocate work efficiently. In environments where employees work remotely or autonomously, monitoring may be presented as the only substitute for direct supervision.
- Security and confidentiality: Monitoring email and internet usage can detect information leakage, prevent intellectual property theft, and identify employees who are sharing confidential information with competitors or unauthorised persons.
- Legal compliance: In regulated industries banking, pharmaceuticals, law employers may be legally required to maintain records of employee communications and transactions. Monitoring is the mechanism through which this compliance is achieved.
- Safety: In manufacturing, construction, and logistics environments, monitoring employee behaviour can identify safety violations and prevent workplace accidents.
- Customer protection: In customer-facing environments, monitoring ensures that employees treat customers appropriately, comply with scripts and protocols, and do not engage in fraudulent or abusive conduct.

C. The Employee Experience

What surveillance feels like from the employee's perspective is an underexamined dimension of the debate. Research on the psychological impact of workplace surveillance consistently reveals:

- Increased anxiety and stress: Employees who know they are being monitored report higher levels of anxiety and stress, particularly when monitoring is continuous and comprehensive.
- Reduced trust: Surveillance signals distrust, and employees respond by trusting their employers less reducing their commitment, engagement, and willingness to raise concerns.
- Chilling effect on communication: When employees know that their communications are monitored, they become more guarded, less willing to raise concerns, less likely to engage in creative or unconventional thinking, and less likely to communicate with colleagues about workplace problems including harassment and discrimination.
- Loss of dignity: Pervasive monitoring particularly monitoring that tracks bathroom breaks, measures keystroke frequency, or requires employees to keep cameras on at home is experienced by many employees as a fundamental violation of dignity.
- Exploitation of data: Employees reasonably fear that data collected through surveillance will be used against them in performance reviews, disciplinary proceedings, or termination decisions often in ways that are opaque and unchallengeable.

These are not trivial concerns. The psychological and dignitary harms of pervasive surveillance are real, and a legal framework that ignores them in favour of employer convenience fails to take seriously the human experience of work.

THE EXISTING LEGAL LANDSCAPE: AN HONEST ASSESSMENT

A. Constitutional Foundation: The Right to Privacy

[1079] Ruth Dukes and Wolfgang Streeck, Labour Constitutions and Surveillance Capitalism (2021) 50(3) Industrial Law Journal 293.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The most important legal development relevant to workplace surveillance is the Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India (2017). The nine-judge bench unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution, overruling earlier decisions that had held otherwise. Justice D.Y. Chandrachud's judgment is which one of six concurring opinions are articulated a rich understanding of privacy that is directly relevant to the workplace context: "Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and dignity and recognises the ability of the individual to control vital aspects of her or his life. Personal choices governing a way of life are intrinsic to privacy." The judgment also specifically addressed informational privacy: "An individual's right to control the dissemination of information about her or his personal life is an aspect of the right to privacy." The Puttaswamy decision establishes the constitutional foundation for employee privacy claims against surveillance. But the decision arose in the context of state action specifically the Aadhaar scheme and its application to private employer conduct requires additional analysis. The Constitution's fundamental rights provisions generally protect against state action, not private action. However, Article 21 has been interpreted to impose positive duties on the state to protect individuals' privacy even against private violations. Moreover, the Puttaswamy judgment's emphasis on dignity and autonomy as the basis of the right to privacy suggests that these values should permeate all legal relationships, including employment.

B. The Information Technology Act, 2000 and Amendment

The Information Technology Act, 2000 (IT Act) and the Information Technology (Amendment) Act, 2008 contain provisions relevant to data protection and privacy, but they were not designed for the employment context and address workplace surveillance only obliquely.

- Section 43A of the IT Act, inserted by the 2008 amendment, requires body corporates that possess or deal with sensitive personal data to maintain reasonable security practices and procedures.[1080] Sensitive personal data is defined under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to include passwords, financial information, health data, sexual orientation, and biometric data.[1081]
- Section 72A of the IT Act creates criminal liability for disclosure of information in breach of contract.[1082]This provision could potentially apply to employers who disclose employee data collected through surveillance to third parties without authorisation, but its application to workplace surveillance is uncertain. The IT Act's framework is inadequate for addressing workplace surveillance for several reasons: it focuses on data security rather than data collection limits; it does not address the employment relationship specifically; it does not establish rights for individuals to access, correct, or restrict processing of their data; and its enforcement mechanism is cumbersome and rarely used. [1083]

C. The Digital Personal Data Protection Act, 2023

After years of legislative limbo, India finally enacted the Digital Personal Data Protection Act, 2023 (DPDPA).[1084] This legislation establishes a comprehensive framework for the processing of personal data, including data collected through workplace surveillance.

[1080] The Information Technology (Amendment) Act, 2008, Section 43A.

[1081] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3.
[1082] The Information Technology Act, 2000, Section 72A
[1083] Srikrishna Committee, supra note 5, pp. 67-89.
[1084] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Key provisions relevant to the employment context include:

- Notice and Consent (Section 6): Data fiduciaries (including employers) must give data principals (including employees) a clear and plain language notice of the data being collected, the purposes for which it is collected, and the manner in which they can exercise their rights. Consent must be free, specific, informed, unconditional, and unambiguous.
- Purpose Limitation (Section 6(1)): Personal data may be processed only for the specific purpose for which consent was given.
- Data Principal Rights (Sections 11-13): Individuals have the right to access information about their data, correct inaccurate data, and seek erasure of data that is no longer necessary.
- Data Fiduciary Obligations (Section 8): Employers must implement appropriate technical and organisational measures to protect personal data, appoint a Data Protection Officer, and ensure that data processors they engage comply with the Act.[28]

However, the DPDPA has significant limitations in the employment context:

- Consent in Employment: The requirement of free and informed consent is problematic in the employment context, where the power imbalance between employer and employee means that consent to monitoring conditions may be a precondition of employment rather than a genuine choice. The Act does not specifically address this power imbalance.
- Legitimate Uses Exception: The Act permits processing without consent for certain "legitimate uses," including employment-related processing. This exception could be interpreted broadly to permit extensive surveillance without requiring employee consent.
- Rules Not Yet Notified: As of early 2024, the rules under the DPDPA have not been notified, leaving the framework incomplete and inapplicable in practice.

D. Labour Laws: A Conspicuous Silence

India's extensive body of labour legislation: the Industrial Disputes Act, 1947; the Factories Act, 1948; the Contract Labour (Regulation and Abolition) Act, 1970; and the four Labour Codes of 2019-20 is conspicuously silent on workplace surveillance. None of these statutes addresses an employer's right to monitor employees, the limits of permissible surveillance, employees' right to privacy within the workplace, or the procedural requirements for introducing surveillance systems. The Factories Act contains provisions on working conditions, health, and safety, but does not address monitoring. The Labour Codes, enacted as recently as 2020, similarly contain no surveillance-specific provisions.[1085] This silence is not accidental it reflects the vintage of India's primary labour legislation, most of which was enacted before the digital revolution made workplace surveillance technically feasible. But it creates a significant gap: the legal framework that governs the employment relationship has nothing to say about one of the most significant developments in the modern employment relationship.

E. Standing Orders and Employment Contracts

In the absence of specific legislation, workplace surveillance is typically governed by:

- Model Standing Orders under the Industrial Employment (Standing Orders) Act, 1946 address conditions of employment including working hours, attendance, and misconduct, but do not address surveillance. [1086]

[1085] The Code on Wages, 2019; The Industrial Relations Code, 2020; The Code on Social Security, 2020; The Occupational Safety, Health and Working Conditions Code, 2020.
[1086] The Industrial Employment (Standing Orders) Act, 1946, Schedule I.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- Employment contracts and HR policies typically contain provisions authorising employer monitoring of company systems, communications, and equipment. Employees are usually required to sign consent forms as a condition of employment. Courts have generally upheld these contractual provisions, treating employee consent however coerced by economic necessity as sufficient legal basis for surveillance.[1087]
- Company CCTV policies in some organisations specify where cameras are placed, how long footage is retained, and who has access. But these policies are internal instruments that employers can modify at will, without employee consultation or regulatory oversight.

The reliance on employment contracts and internal policies as the primary governance mechanism for workplace surveillance is deeply problematic. Contractual consent in the employment context is inherently compromised by power imbalance: an employee who objects to surveillance terms in a job offer has little practical choice but to accept them or forgo employment. Treating such consent as equivalent to the voluntary consent that justifies data processing in other contexts ignores the realities of labour markets. [1088]

THE JUDICIARY: JUDICIAL ENGAGEMENT WITH SURVEILLANCE DISPUTES

A. Limited but Emerging Jurisprudence:

Indian courts have dealt with workplace surveillance issues in a limited number of cases, without developing a comprehensive or consistent jurisprudence. The cases that exist tend to arise in specific factual contexts—disciplinary proceedings where surveillance evidence is challenged, or wrongful termination cases where employees contest the basis of employer decisions.

B. Key Cases

In **Sharda v. Dharmpal (2003)**,[1089]the Supreme Court held that in matrimonial proceedings, the right to privacy is not absolute and must be balanced against other interests. While not a workplace case, this decision established the principle that privacy rights can be overridden when other legitimate interests are at stake a principal court have applied in employment contexts.

In **Canara Bank v. Canara Sales Corporation (1987)**,[1090] the Supreme Court recognised that employers have legitimate interests in monitoring employee conduct, particularly where there is suspicion of misconduct. The Court upheld disciplinary action based on covert monitoring of an employee suspected of financial irregularities.

In **Mr. X v. Hospital Z (1998),**[1091]the Court held that the right to privacy is not absolute and may yield to other legitimate interests including the interests of third parties. This principle has been cited in employment contexts to justify employer surveillance on grounds of business necessity.

More recently, in the context of gig worker management, the Delhi High Court in **India Federation of App-based Transport Workers v. Union of India (2021)**[1092]considered the algorithmic management practices of platform companies. While the Court did not specifically address privacy, it acknowledged the significance of algorithmic control over worker behaviour a form of surveillance-based management and directed the government to consider appropriate regulatory responses.

C. The Gap in Constitutional Application

The most significant judicial gap is the absence of a clear ruling on whether the Puttaswamy right to privacy protects employees against employer surveillance in the private sector. The

[1087] Suresh C. Srivastava, Industrial Relations and Labour Laws (Vikas Publishing House, 6th edn., 2019), pp. 234-256.
[1088] Mark Freedland and Nicola Kountouris, The Legal Construction of Personal Work Relations (Oxford University Press, 2011), pp. 289-312.
[1089] Sharda v. Dharmpal, (2003) 4 SCC 493
[1090] Canara Bank v. Canara Sales Corporation, AIR 1987 SC 1603.
[1091] Mr. X v. Hospital Z, (1998) 8 SCC 296.
[1092] Indian Federation of App-based Transport Workers v. Union of India, W.P.(C) 1068/2021 (Delhi High Court).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Constitutional right to privacy under Article 21 operates primarily against state action. For employees of private companies, the right to privacy must be vindicated through statutory protections which, as this article has demonstrated, are inadequate or through the development of common law principles which Indian courts have not yet undertaken in a systematic way. This gap needs to be filled, either by legislation or by judicial creativity. Some High Courts have gestured toward a more robust protection of employee privacy recognising, for example, that employees do not entirely surrender their right to dignity upon entering employment but a definitive Supreme Court ruling on employee privacy in the workplace is still awaited.

SECTOR-SPECIFIC SURVEILLANCE: PARTICULAR CONCERNS

A. Gig Workers: Algorithmic Surveillance

Platform workers experience the most intensive and consequential form of workplace surveillance algorithmic management. Every aspect of a gig worker's engagement with a platform is monitored, scored, and fed into algorithms that determine work allocation, pricing, and continued access to the platform. A delivery executive on Swiggy or Zomato knows that her acceptance rate, delivery time, customer rating, cancellation rate, and online hours are all continuously monitored. A driver on Uber knows that his rating, trip acceptance rate, cancellation rate, and navigation compliance are tracked. These metrics determine whether a worker receives premium assignments, whether she is eligible for bonuses, and ultimately whether her account is deactivated.

This surveillance is particularly problematic because:

1. It is opaque: Workers do not know exactly what is being measured, how metrics are weighted, or how algorithmic decisions are made
2. It is unappealable: Algorithmic decisions are difficult to challenge because the basis of the decision is hidden in proprietary code
3. It creates perverse incentives: Workers optimise for measured metrics rather than genuine quality of service
4. It enables unilateral termination: A worker's account can be deactivated based on algorithmic scoring without human review, explanation, or meaningful remedy[1093]

The Code on Social Security, 2020 recognised platform workers as a distinct legal category but said nothing about algorithmic management or surveillance. The regulatory vacuum in this area leaves millions of gig workers entirely without protection.[1094]

B. Call Centres and BPO: Total Surveillance

India's large and growing business process outsourcing (BPO) and call centre industry operates under conditions of extremely intensive surveillance. Employees' calls are recorded, their screens are monitored, their keystrokes are logged, their adherence to scripts is tracked, their performance metrics are calculated in real time, and their bathroom breaks may be timed. This level of monitoring is justified by employers on grounds of quality control, client contractual requirements, and compliance. But research on BPO employees consistently documents high levels of stress, burnout, and psychological harm associated with working in conditions of total surveillance. The workers who bear the burden of this surveillance young, typically from lower-middle-class backgrounds, often women have limited bargaining power and few alternatives. The take-it-or-leave-it nature of employment in this sector means that consent to surveillance is a precondition of employment, not a genuine choice.

[1093] Jeremias Prassl, Humans as a Service (Oxford University Press, 2018), pp. 67-89.
[1094] The Code on Social Security, 2020, Sections 2(35) and 2(77).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

C. Factory Workers: Biometric and Physical Monitoring

Manufacturing workers increasingly face biometric attendance monitoring, CCTV surveillance on the shop floor, and in some cases wearable devices that track their movement, posture, and physical condition. Biometric data collection raises particular privacy concerns because biometric data fingerprints, facial geometry, iris patterns—is uniquely personal, cannot be changed if compromised, and has uses well beyond attendance management. An employee who provides biometric data to an employer is providing something far more sensitive than a password or an employee number, yet the legal protections applicable to biometric data in the employment context are minimal.

D. White-Collar Workers: Remote Monitoring

The COVID-19 pandemic brought surveillance into the homes of white-collar workers in ways that had not previously been experienced. Employers who adopted remote monitoring tools requiring workers to keep cameras on, installing screenshot software, tracking mouse movement effectively extended the workplace into employees' personal spaces. This extension of surveillance into the home is qualitatively different from workplace monitoring. The home has always been regarded as the most private of spaces a sanctuary from the demands and scrutiny of professional life. Remote monitoring breaks down this boundary, subjecting the domestic environment to the employer's gaze in ways that raise profound questions about the right to privacy, the right to family life, and the limits of employment authority.

COMPARATIVE PERSPECTIVES: HOW OTHER JURISDICTIONS HAVE APPROACHED WORKPLACE SURVEILLANCE

A. European Union: The GDPR Framework

The European Union's General Data Protection Regulation (GDPR), which came into force in 2018, provides the most comprehensive framework for employee data protection in the world. While not specifically a workplace surveillance law, the GDPR's principles apply fully to employer processing of employee data.[1095]

Key GDPR principles relevant to workplace surveillance include:

- Lawfulness, Fairness, and Transparency: Employers must have a lawful basis for processing employee data, must process it fairly, and must be transparent about what is collected and why.
- Purpose Limitation**: Data collected for one purpose (say, time and attendance management) cannot be used for a different purpose (say, performance evaluation) without additional justification.
- Data Minimisation: Employers may collect only the data that is actually necessary for the stated purpose. This principle directly limits the scope of surveillance—if the purpose is attendance management, collecting detailed biometric data is disproportionate; a simple electronic badge system might suffice.
- Special Category Data: Biometric data used for identification purposes is classified as a "special category" requiring explicit consent or a specifically identified legal basis. This places significant constraints on biometric surveillance.
- Employee Rights: Employees have rights to access their data, to correct inaccuracies, to restrict processing, and in some circumstances to object to processing. These rights give employees meaningful control over information about themselves.

The GDPR's consent requirement is particularly important in the employment context. GDPR guidance from the Article 29 Working Party

[1095] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119/1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

(now the European Data Protection Board) has noted that genuine consent is difficult to achieve in employment relationships given the power imbalance, and has urged employers to rely on other lawful bases such as necessity for performance of the contract or legitimate interests rather than claiming consent that may not be freely given.[1096] Individual EU member states have enacted additional provisions. Germany's Works Constitution Act requires consultation with workers' councils before introducing surveillance systems. France's Labour Code requires prior consultation with employee representatives and notification to the national data protection authority before implementing monitoring systems. The Netherlands requires notification to affected employees of any monitoring system.[1097]

B. United Kingdom: A Balancing Act

The United Kingdom, applying the GDPR framework through the UK GDPR and Data Protection Act, 2018, has developed detailed guidance on workplace monitoring through the Information Commissioner's Office (ICO).[1098]

The ICO's guidance establishes that:

- Employers must inform employees about monitoring before it takes place
- Monitoring must be proportionate to the business need
- Covert monitoring can only be justified in exceptional circumstances where there is specific evidence of serious wrongdoing
- Monitoring personal communications requires stronger justification than monitoring work communications
- Employees' reasonable expectation of privacy must be respected even in the workplace

The key concept of reasonable expectation of privacy is particularly important. British courts and tribunals have held that employees retain some degree of privacy even in the workplace—they do not surrender all privacy rights upon entering employment. The extent of this residual privacy depends on context: an employee in an open-plan office has a lower expectation of privacy than an employee in a private office; communications made through a personal device have higher privacy protection than those made through a company device.[1099]

C. United States: A Patchwork Approach

The United States lacks federal legislation specifically governing workplace surveillance, relying instead on a patchwork of constitutional provisions (applicable only to government employers), federal statutes, and state laws. The Electronic Communications Privacy Act (ECPA), 1986 regulates interception of electronic communications but contains a significant exception for employer monitoring of company systems effectively allowing employers to monitor employee communications made through company equipment and systems. Several US states have enacted more protective legislation. Connecticut and Delaware require employers to provide written notice before monitoring employee internet usage and email. Illinois prohibits the use of artificial intelligence in employment video interviews without specific disclosure and consent. New York City requires employers to notify workers of automated employment decision tools used in hiring. The US approach illustrates both the possibilities and limitations of addressing workplace surveillance through fragmented state-level legislation without a comprehensive federal framework.

D. Germany: Co-determination as Protection

Germany's approach to workplace surveillance is distinctive because of the role of workers' councils in workplace governance. Under the Works Constitution Act, workers' councils have co-determination rights on matters affecting employee behaviour, performance, and working

[1096] Article 29 Working Party (now European Data Protection Board), Opinion 2/2017 on Data Processing at Work (WP 249, June 8, 2017).

[1097] Works Constitution Act, 1972 (Germany), Section 87(1)(6); French Labour Code, Articles L. 1121-1 and L. 2323-32.

[1098] Data Protection Act, 2018 (UK); UK General Data Protection Regulation (UK GDPR).

[1099] Halford v. United Kingdom [1997] ECHR 32 (European Court of Human Rights); Barbulescu v. Romania [2017] ECHR 742 (Grand Chamber).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

conditions including the introduction of technical surveillance systems.[1100] Before an employer can introduce a surveillance system CCTV, computer monitoring, biometric systems it must negotiate with the workers' council and obtain its agreement. If agreement cannot be reached, the matter goes to arbitration. This gives workers genuine collective power to limit or shape surveillance before it is implemented a fundamentally different approach from the individual consent model that most other jurisdictions rely upon. The German model is instructive because it treats workplace surveillance as a collective concern requiring collective negotiation, rather than as an individual privacy matter to be addressed through personal data protection rights. This collective dimension is often absent from privacy-focused approaches to surveillance regulation.

E. Lessons for India

The comparative analysis reveals several principles that could inform Indian regulatory development:

- Transparency: Employees should be informed about what is monitored, how data is used, and who has access before monitoring begins, not buried in employment contract fine print.
- Proportionality: The scope and intensity of surveillance should be proportionate to the business purpose an employer cannot justify comprehensive surveillance of all employee communications on the basis of occasional security concerns.
- Purpose limitation: Data collected for one purpose should not be used for other purposes without additional justification.
- Collective negotiation: Trade unions and workers' representatives should have a role in determining surveillance policies surveillance is a collective workplace issue, not just an individual privacy matter.
- Special protection for sensitive data: Biometric data requires heightened protection and should only be collected where genuinely necessary.
- Covert surveillance restrictions: Covert monitoring should be permitted only in exceptional circumstances with appropriate authorisation.

THE CONSTITUTIONAL DIMENSION: PRIVACY, DIGNITY, AND EMPLOYER POWER

A. Privacy as a Fundamental Right in the Workplace

The Puttaswamy judgment established that privacy is a fundamental right, but it did not specifically address whether this right extends to the employment relationship between private parties. This question requires careful constitutional analysis. The traditional view is that constitutional rights operate vertically against the state not horizontally against private parties. But Indian constitutional jurisprudence has progressively recognised horizontal application of rights in certain contexts. The Supreme Court has held that private employers exercising significant economic power may be subject to constitutional constraints in contexts involving fundamental rights.[1101] More significantly, the Puttaswamy judgment emphasised that privacy is grounded in human dignity a value that permeates all legal relationships. Justice Chandrachud observed: "Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and offers a guarantee of a rational zone to every individual."If privacy is grounded in dignity, and if dignity is a value that must be respected in all human relationships, then the employment relationship where human beings spend a significant portion of their lives cannot be exempt from its demands.

[1100] Works Constitution Act, 1972 (Germany), Section 87(1)(6).

[1101] Zee Telefilms Ltd. v. Union of India, (2005) 4 SCC 649 (horizontal application of constitutional rights).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

B. The Right to Work and Dignity

Article 21's protection of life with dignity has been interpreted to include the right to livelihood.[1102] If employees can only obtain livelihood by surrendering their dignity through acceptance of invasive surveillance, there is a tension within Article 21 itself the right to livelihood being purchased at the cost of the dignity that the right to life is supposed to protect. This tension supports the development of a legal framework that enables employees to earn their living without surrendering their privacy and dignity that treats some minimum privacy protection as a condition of the employment relationship that cannot be contracted away.

C. Directive Principles and State Obligations

The Directive Principles of State Policy impose obligations on the state to ensure just and humane conditions of work under Article 42 and to protect workers from conditions that are injurious to health and dignity under Article 39. Pervasive surveillance that causes psychological harm and violates dignity arguably engages these obligations, requiring the state to legislate appropriate protections.[1103]

TOWARDS A FRAMEWORK FOR WORKPLACE SURVEILLANCE REGULATION IN INDIA

The analysis in this article points toward the need for a comprehensive legislative framework governing workplace surveillance. The following principles should guide its development.

A. Core Principles

- Transparency and Prior Notice: Employers should be required to inform employees, before employment commences and before any new surveillance system is introduced, of:

- The nature and scope of surveillance

- The purpose for which data is collected

- How long data will be retained

- Who will have access to collected data

- How data will be used in employment decisions

- Employees' rights regarding their data

- Proportionality: Surveillance must be proportionate to the business purpose. An employer cannot justify comprehensive monitoring of all employee activities on the basis of a specific, limited security concern. The least invasive means of achieving the legitimate purpose should be used.
- Purpose Limitation: Data collected for one purpose attendance management, for example cannot be used for another purpose performance evaluation without separate justification and, where appropriate, employee notification.
- Prohibition on Covert Surveillance: Covert surveillance should be prohibited except in exceptional circumstances specifically, where there is reasonable suspicion of serious criminal conduct and where overt surveillance would compromise the investigation. Even covert surveillance should require prior authorisation from an independent authority.
- Special Protection for Sensitive Data: Biometric data, health data, and location data require heightened protection. Biometric systems should only be used where the purpose cannot be achieved through less invasive means, and biometric data should never be shared with third parties without explicit consent.
- Employee Rights: Employees should have the right to access data collected about them, to correct inaccurate data, to know how their data has been used in employment decisions, and to challenge decisions made solely on the basis of automated processing.

B. Sector-Specific Provisions

[1102] Olga Tellis v. Bombay Municipal Corporation, AIR 1986 SC 180.
[1103] Constitution of India, Articles 39 and 42.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- Gig Workers and Algorithmic Management: Platform companies should be required to disclose the parameters of algorithmic management systems to workers, explain the basis of algorithmic decisions affecting their access to work and earnings, provide human review of deactivation decisions, and ensure that algorithmic systems do not discriminate on protected grounds.[1104]
- Remote Work Monitoring: Employers who monitor remote workers should be required to: limit monitoring to working hours; refrain from monitoring personal devices; refrain from accessing domestic environments through cameras or screen monitoring without specific consent; and provide remote workers with the same privacy protections as office-based workers.
- BPO and Call Centres: Quality monitoring in call centres should be subject to clear protocols, disclosed to employees in advance, limited to what is necessary for quality and compliance purposes, and should not be used punitively without fair process.

C. Institutional Framework

- Labour Courts and Employment Tribunals: Disputes about workplace surveillance should be ad judicable by labour courts or specialist employment tribunals with expertise in employment law and data protection.
- Data Protection Authority: The Data Protection Board established under the DPDPA should have specific jurisdiction over employment data processing, with power to investigate complaints, issue guidance, and impose penalties.
- Workers' Councils and Trade Union Rights: Where employees have elected representatives or trade union representation, employers should be required to consult them before introducing new surveillance systems drawing on the German model.
- Labour Inspectorate: Labour inspectors should be empowered and trained to assess employers' surveillance practices as part of routine inspection processes.

D. Collective Bargaining

Surveillance policies should be a mandatory subject of collective bargaining in workplaces where unions are recognised. Workers' collective knowledge of workplace conditions and collective bargaining power provide the most effective counterbalance to employer surveillance authority. [1105]

RECOMMENDATIONS

1. Transparency in Workplace Surveillance: Employers should clearly inform employees about the nature, purpose, and extent of monitoring to ensure fairness and avoid hidden surveillance practices.
2. Proportionality Principle: Surveillance should be limited to what is necessary for business needs and should not be excessive or intrusive into employees' personal space.
3. Protection of Employee Privacy Rights: Employees must retain their fundamental right to privacy and dignity even within the workplace, as recognized in Justice K.S. Puttaswamy v. Union of India.
4. Regulation of Biometric and Sensitive Data: Strict safeguards should be applied when collecting biometric or personal data to prevent misuse and unauthorized access.
5. Employee Consent and Awareness: Consent should be informed and meaningful, ensuring employees understand how their data is being used.
6. Limits on Remote Work Monitoring: Monitoring in work-from-home settings

[1104] NITI Aayog, India's Booming Gig and Platform Economy (June 2022), pp. 56-67.

[1105] Kamala Sankaran, Labour Law in South Asia: The Unfinished Agenda (ILO, Geneva, 2014), pp. 112-134.

should respect personal boundaries and avoid intrusion into private life.

7. Algorithmic Transparency in Gig Work: Platform workers should be informed about how algorithms affect their ratings, work allocation, and job security.
8. Strengthening Labour Law Framework: Existing labour laws should be updated to include provisions specifically addressing workplace surveillance.
9. Right to Access and Correction of Data: Employees should have the right to view, correct, and challenge the data collected about them.
10. Legal Enforcement and Accountability: Authorities should enforce strict penalties for misuse of employee data and ensure proper grievance redressal mechanisms.

CONCLUSION

There is something important at stake in the question of workplace surveillance that goes beyond data protection, beyond labour law, and beyond the technicalities of consent frameworks and proportionality tests. It is about what we think work is—and what we think workers are. If workers are simply inputs to a production process, to be managed, optimised, and monitored like any other input, then comprehensive surveillance is a rational management tool and the only question is its technical efficiency. But if workers are human beings who bring not just their labour but their dignity, their creativity, their relationships, and their full humanity to their working lives, then the manner in which they are monitored matters profoundly not just legally but morally. The Supreme Court's Puttaswamy judgment understood this. It recognised that privacy is not a bureaucratic technicality but a condition of human dignity of the individual's ability to shape her own life, control information about herself, and maintain the inner freedom that authoritarian surveillance corrodes. A workplace in which every keystroke is logged, every movement tracked, and every communication scanned is a workplace in which this inner freedom is diminished even if the employee has "consented" to it as a condition of her employment. India is at a crossroads in the regulation of workplace surveillance. The technological tools for surveillance have never been more sophisticated or more accessible to employers. The legal protections for employees have never been more inadequate relative to the surveillance capabilities that employers can deploy. The Puttaswamy judgment provided a constitutional foundation; the Digital Personal Data Protection Act, 2023 provides a starting framework. But neither, alone, is sufficient to protect employees from the surveillance revolution that is reshaping their working lives. What is needed is a comprehensive, principled, and practically effective legal framework one that acknowledges legitimate employer interests in supervision, safety, and compliance, while also recognising that employees do not surrender their humanity, dignity, and privacy when they cross the threshold of their workplace. Building that framework is the urgent legislative and judicial task that this article has attempted to define. The workplace of the future will be shaped by technology in ways that are impossible to fully predict. But the values that should govern it dignity, fairness, transparency, and respect for the human person are not difficult to identify. Translating those values into law is the challenge that Indian policymakers, judges, and advocates must now confront.

REFERENCES

- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Information Technology Act, 2000 (Act No. 21 of 2000)
- The Information Technology (Amendment) Act, 2008
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- The Code on Wages, 2019
- The Industrial Relations Code, 2020
- The Code on Social Security, 2020

- The Occupational Safety, Health and Working Conditions Code, 2020
- Regulation (EU) 2016/679 (General Data Protection Regulation)
- Data Protection Act, 2018 (United Kingdom)
- Works Constitution Act, 1972 (Germany)
- Electronic Communications Privacy Act, 1986 (United States)
- Constitution of India
- Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019)
- Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018)
- Jeremias Prassl, Humans as a Service (Oxford University Press, 2018)
- Kamala Sankaran, Labour Law in South Asia (ILO, Geneva, 2014)
- Mark Freedland and Nicola Kountouris, The Legal Construction of Personal Work Relations (Oxford University Press, 2011)
- Suresh Vasudevan, Data at Work: Surveillance in India's Call Centres (2019) 54(22) Economic and Political Weekly 34
- Ruth Dukes and Wolfgang Streeck, Labour Constitutions and Surveillance Capitalism (2021) 50(3) Industrial Law Journal 293
- Prem Sikka, Employment Relations and Surveillance (2018) 49(4) Industrial Relations Journal 345
- Niels van Doorn, Platform Labor (2017) 4(1) Information, Communication & Society 898

INSTITUTE OF LEGAL EDUCATION

(Managed by I.L.E. EDUCATIONAL TRUST)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344