

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

WORKPLACE SURVEILLANCE OF GOVERNMENT SERVANTS: PRIVACY, PROPORTIONALITY AND CONSTITUTIONAL LIMITS ON DIGITAL MONITORING

AUTHORED BY - SHIYAM A

Abstract

The digitisation of public administration has brought wider use of biometric attendance systems, CCTV, GPS-based field monitoring, logs generated by official devices, email inspection and algorithmic tools for assessing performance. These technologies may improve service delivery, cybersecurity and accountability. At the same time, they can generate detailed records of employees' conduct that are capable of continuous collection and subsequent use for purposes beyond those originally contemplated. This paper examines the constitutional limits of digital workplace surveillance of government servants in India. It argues that public employment does not remove the protection of privacy and that intrusive monitoring must be supported by lawful authority and justified by a legitimate purpose. It must also be suitable, necessary and proportionate in the strict sense, with safeguards adequate to prevent misuse. The analysis brings together Supreme Court jurisprudence on privacy and proportionality, data-protection legislation, public-service obligations and comparative human-rights standards. Its principal contribution is a proposed framework for constitutional review that distinguishes routine administrative logging from more intrusive forms of surveillance and considers system design, data handling throughout its lifecycle and the employment consequences of monitoring. Properly limited surveillance may help protect public resources without undermining constitutional legitimacy.

Keywords: government servants; workplace surveillance; right to privacy; proportionality; Article 21; informational privacy; digital monitoring; data protection; public administration.

1. Introduction

Digital systems now play a substantial role in public administration. They are used to record attendance, verify identity, secure government networks and monitor the delivery of public services. Biometric scanners, CCTV, GPS-enabled field applications, access logs and productivity analytics may help departments address absenteeism, protect confidential

information and investigate suspected misconduct. Yet the same systems can accumulate extensive information about employees' movements, communications and work patterns. When these records are combined, they may reveal behavioural patterns well beyond the immediate purpose for which the information was collected.

The constitutional issue is not whether government departments may supervise their employees. Public servants remain subject to lawful service conditions, attendance requirements, confidentiality duties and disciplinary rules. The more difficult question is when supervision becomes an unjustified or disproportionate interference with privacy, dignity, autonomy or other fundamental freedoms. Article 21 protects life and personal liberty, Article 14 constrains arbitrary State action, and Article 19 safeguards specified freedoms subject to constitutionally permissible restrictions. These protections remain relevant when the State acts in its capacity as employer rather than as regulator or law-enforcement authority.¹

In *Justice K S Puttaswamy (Retd) v Union of India*, a nine-judge Bench held that privacy is a fundamental right arising from Part III of the Constitution. The decision places informational privacy within the scope of constitutional protection and rejects the view that privacy loses its relevance merely because information is held by another institution. The proportionality principles developed in later cases provide a means of assessing whether a surveillance measure is genuinely justified, rather than simply administratively convenient.²³

The paper proceeds on the basis that digital monitoring by government employers is an exercise of State power and should therefore have a demonstrable legal foundation and a proportionate design. It does not argue that all workplace monitoring should be prohibited. Instead, it supports a graduated approach to scrutiny. Routine attendance records and security logs may be defensible for ordinary administrative purposes, whereas continuous location tracking, inspection of communications content and algorithmic profiling with employment consequences call for stronger justification and more extensive safeguards.

1.1 Research questions and objectives

The study addresses four questions: what protection does the Indian constitutional right to privacy afford government servants in the face of digital monitoring; how should proportionality be applied to commonly used surveillance technologies; what part is played by data-protection legislation and service rules; and which safeguards should govern both

¹Constitution of India, arts 14, 19 and 21.

²*Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

³*K S Puttaswamy (Aadhaar-5J) v Union of India* (2019) 1 SCC 1 [para 319].

surveillance itself and the use of monitoring data in employment decisions? Its objectives are to clarify the relevant constitutional principles, examine leading judicial authorities, identify regulatory gaps and develop a practical framework for review.

1.2 Methodology and scope

This paper adopts a doctrinal methodology, examining constitutional provisions, legislation, reported judgments, international instruments and selected comparative decisions. It does not claim to provide empirical evidence about the prevalence of particular surveillance technologies across Indian government departments. Its focus is monitoring undertaken by government employers and public authorities in India. Private-sector workplace surveillance is considered only where comparative principles assist the analysis of the public-sector context.

2. Literature Review and Original Contribution

Privacy scholarship offers several approaches that help explain the risks associated with workplace surveillance. Daniel J Solove, for example, treats privacy as a set of related problems, including surveillance, aggregation, identification and secondary use. This perspective helps explain how information that appears innocuous in isolation may become intrusive when combined with other records. An attendance log may seem limited in scope, but, when considered alongside location histories, access records and communications metadata, it can reveal patterns that no individual system was designed to disclose.⁴

Helen Nissenbaum's theory of contextual integrity similarly suggests that privacy cannot be understood solely in terms of secrecy or individual control. It also depends on whether information flows are appropriate to the context and to the roles of the parties involved. In government employment, data collected to confirm a field visit should not automatically become available for unrelated personal profiling. The purpose of collection, the nature of the information, the recipient and the conditions governing its transfer are all relevant. This approach helps identify when legitimate accountability gives way to function creep.⁵

Research on quantified work draws attention to the imbalance of power that may arise when employers use data-driven systems to measure, rank or predict employee performance. Ifeoma Ajunwa's work on the quantified worker illustrates how technologies can reduce complex professional activity to measurable indicators, potentially obscuring context and reinforcing

⁴Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008).

⁵Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

unequal power relationships. In the public sector, this concern has an additional constitutional dimension: the employer is also a State authority bound by fundamental rights and public-law obligations.⁶

Indian constitutional jurisprudence has developed the principles of privacy and proportionality largely through disputes concerning State collection of data, identity systems, communications restrictions and other exercises of public power. These decisions establish important foundations, but they do not amount to a comprehensive, technology-specific code for workplace monitoring. Departments still require practical criteria for distinguishing attendance verification from continuous tracking, evaluating less intrusive alternatives, setting retention periods and preventing data collected for one purpose from being used in unrelated employment decisions.

The paper does not claim to introduce privacy or proportionality as new constitutional concepts. Its contribution lies instead in applying established doctrine to the full lifecycle of workplace surveillance. The proposed framework considers the degree of intrusion, the legal basis and stated purpose, the effectiveness of alternatives, safeguards governing the data lifecycle and the consequences of using information against an employee. In this way, broad constitutional principles may be translated into a more consistent method of assessment for policymakers, courts and departmental decision-makers.

3. The Constitutional Foundation

3.1 Article 21 and informational privacy

Article 21 provides that no person may be deprived of life or personal liberty except according to procedure established by law. In *Puttaswamy*, the Supreme Court recognised privacy as a fundamental right closely associated with liberty, dignity and autonomy. The constitutional interest is not confined to physical seclusion. Information about an individual's movements, communications, associations and behaviour may also engage privacy when it is collected, retained, analysed or disclosed.⁷

The employment context may affect the reasonable scope of supervision, but it does not extinguish the underlying right. An employee may have a more limited expectation of privacy when using an official computer for official work, particularly where a clear monitoring policy has been communicated. Nevertheless, the fact that equipment belongs to the State does not

⁶Ifeoma Ajunwa, *The Quantified Worker: Law and Technology in the Modern Workplace* (Cambridge University Press 2023).

⁷*Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

necessarily justify unrestricted inspection of communications or continuous tracking beyond working hours. Permissible monitoring should remain connected to the task being performed and to the legal basis for collecting the information.

3.2 Article 14 and non-arbitrariness

Article 14 requires State action to be non-arbitrary and guards against unjustified differential treatment. Surveillance may raise concerns under this provision where certain employees are monitored more intensively without objective criteria, where the system relies on measures unrelated to their actual duties, or where automated scores influence adverse decisions without adequate explanation. Differences between roles may justify different levels of monitoring, but any distinction should be rational, documented and connected to the operational risks involved.

3.3 Article 19 and chilling effects

Article 19 protects specified freedoms, including freedom of speech and expression, subject to restrictions permitted by the Constitution. Surveillance may discourage lawful expression even where no formal prohibition has been imposed. Employees who believe that their communications or associations are continually observed may be less willing to engage in legitimate professional discussion, express criticism or report wrongdoing. This does not relieve public servants of lawful conduct or confidentiality obligations. It does, however, suggest that monitoring should not be used as an instrument of arbitrary control over constitutionally protected activity.

3.4 Public employment is not a constitutional waiver

Public service entails compliance with lawful duties, but accepting government employment does not amount to a waiver of fundamental rights. The central issue is whether a particular interference is authorised and justified, not simply whether the employee is subject to managerial supervision. General powers to manage the workforce may support ordinary oversight; they should not, without further justification, be treated as authority for every intrusive form of technological monitoring.

4. Proportionality as the Governing Method

The Supreme Court has applied proportionality when assessing restrictions on fundamental rights. *Modern Dental College and Research Centre v State of Madhya Pradesh* is an important authority in this area, while the *Aadhaar Constitution Bench* judgment articulated a four-part

inquiry involving legitimate aim, suitability, necessity and balancing. This approach is useful for workplace surveillance because it requires scrutiny of both the objective pursued and the means selected to achieve it.⁸⁹

4.1 Legitimate purpose

A department should identify the specific objective for which monitoring is proposed. Examples may include verifying attendance, protecting a government network, securing a sensitive facility, confirming an authorised field assignment or investigating a credible allegation of misconduct. General appeals to 'efficiency' or 'discipline' do not, by themselves, establish necessity. The authority should explain the problem it seeks to address, the basis for believing monitoring is needed and the relationship between the information collected and the stated objective.

4.2 Suitability

A monitoring system must be capable of advancing the objective relied upon to justify it. Biometric authentication may help prevent impersonation at attendance points, while network logs may assist in identifying unauthorised access. Keyboard activity, by contrast, may provide a poor indication of the quality of legal research, policy analysis or public-facing work. Where a system generates misleading indicators, its suitability may be open to question.

4.3 Necessity and less intrusive alternatives

The authority should also consider whether the same objective could reasonably be achieved through a less intrusive measure that is equally effective. Attendance might be verified through a limited check-in system rather than continuous location tracking. A suspected cyber incident could initially be examined through access logs and a targeted review, rather than by inspecting every employee's communications. Alternatives must be assessed in light of practical circumstances, but any decision to adopt a more intrusive approach should be supported by reasons and recorded.

4.4 Balancing and cumulative effects

At the balancing stage, the importance of the objective must be weighed against the effect on rights. Relevant considerations include the sensitivity of the information, the number of

⁸Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.

⁹K S Puttaswamy (Aadhaar-5J) v Union of India (2019) 1 SCC 1.

employees affected, the duration and frequency of monitoring, the reliability of the data, the risk of misuse, access controls, retention practices, potential secondary uses and the consequences for employment. The combined effect of several systems is especially important. Data points that appear modest when considered separately may, once aggregated, produce a detailed profile of an employee's behaviour.

4.5 Procedural safeguards as part of proportionality

Proportionality should be assessed across the monitoring process, not solely at the moment information is collected. Prior notice, restricted access, deletion schedules, audit trails, human review and effective remedies may reduce the degree of interference. Such safeguards cannot make an unlawful or inherently excessive measure valid, but they are relevant to determining whether a system is proportionate in both design and operation.

5. Judicial Authorities

5.1 Puttaswamy (2017)

In Justice K S Puttaswamy (Retd) v Union of India, a nine-judge Bench unanimously recognised privacy as a fundamental right. The decision provides the starting point for constitutional analysis of digital monitoring in India. It supports the view that informational privacy may be implicated even where the State does not physically intrude into a person's home. The judgment does not set out a detailed code for workplace surveillance; its principles must instead be applied to the features and effects of the particular system under consideration.

5.2 Puttaswamy (Aadhaar) (2019)

The Aadhaar Constitution Bench considered biometric identity infrastructure and the limits of State use of identity information. Its proportionality analysis is relevant to biometric attendance and authentication systems. However, the outcome of the Aadhaar litigation should not be interpreted as blanket approval of every biometric arrangement. The legality of biometric processing in a workplace depends on the purpose pursued, the authority relied upon, the system's design, the safeguards provided and the applicable statutory context.

5.3 Modern Dental College (2016)

Modern Dental College concerned State regulation of admissions and fees in professional educational institutions, rather than workplace surveillance. Its relevance here is doctrinal: the decision contributes to the Supreme Court's proportionality jurisprudence. It should therefore

be cited as a general constitutional authority, not as a case that directly decided the legality of employee monitoring.

5.4 Anuradha Bhasin (2020)

Anuradha Bhasin v Union of India concerned restrictions on internet and communications services in Jammu and Kashmir. The Court considered the constitutional consequences of restrictions affecting freedom of speech and professional activity, and emphasised the importance of legal and procedural scrutiny of the relevant orders. Although the case did not concern employee surveillance, it may inform analysis by analogy where State action limits digital activity or affects the exercise of constitutional freedoms.¹⁰

5.5 Bărbulescu v Romania (2017)

In Bărbulescu v Romania, the Grand Chamber of the European Court of Human Rights considered an employer's monitoring of workplace communications under Article 8 of the European Convention on Human Rights. It found that the domestic courts had not adequately balanced the employee's privacy interests against those of the employer. The factors identified included advance notice, the scope and intensity of monitoring, the reasons for accessing communications content, the availability of less intrusive alternatives, the consequences for the employee and the safeguards in place. The decision is not binding precedent in India, but it offers a useful comparative framework.¹¹

5.6 What the authorities do—and do not—establish

Taken together, these authorities support the protection of privacy, the use of proportionality and the importance of procedural scrutiny. They do not establish that all employee monitoring is unlawful, nor has the Supreme Court adopted a single rule that governs every workplace technology. The framework advanced here is a proposed application of existing constitutional doctrine, rather than a claim that Indian courts have already developed a comprehensive surveillance code.

6. Statutory and Administrative Framework

6.1 Digital Personal Data Protection Act 2023: commencement matters

The Digital Personal Data Protection Act 2023 is relevant to identifiable digital records

¹⁰Anuradha Bhasin v Union of India (2020) 3 SCC 637.

¹¹Bărbulescu v Romania App no 61496/08 (ECtHR, 5 September 2017).

generated through workplace monitoring. Its commencement, however, is phased. Notification GSR 843(E), dated 13 November 2025, brought certain provisions into force immediately, deferred section 6(9) and section 27(1)(d) for one year, and postponed sections 3–5, most provisions in sections 6–17 and other specified provisions for eighteen months. On the basis of that notification, and as at 22 October 2026, the core processing provisions in sections 3–17 have not yet commenced; the general eighteen-month date is 13 May 2027, unless a later notification changes that position. The Gazette should be checked again before publication.¹² The Digital Personal Data Protection Rules 2025 also provide for phased commencement. Rule 1 states that rules 1, 2 and 17–21 commenced on publication; rule 4 is scheduled to commence after one year; and rules 3, 5–16, 22 and 23 are scheduled to commence after eighteen months. It would therefore be inaccurate, at the date of this manuscript, to suggest that all substantive obligations under the Act and Rules are already operational. Their application, including the relevant grounds for processing, exemptions and provisions concerning government bodies, must be assessed by reference to the precise statutory text and commencement dates.¹³ The phased commencement of the regime gives departments a reason to prepare appropriate governance arrangements before the core processing provisions take effect. This paper does not treat the Act as the sole source of privacy protection. Articles 14, 19 and 21 continue to provide an independent constitutional framework, subject to the doctrine applicable to the particular facts.

6.2 Service rules and departmental policies

Government servants are subject to the service rules, conduct rules, disciplinary procedures and lawful administrative instructions applicable to their posts. These instruments may require punctual attendance, appropriate use of official systems and protection of confidential information. The substantive duty and the method used to enforce it must nevertheless be considered separately. A requirement to attend work does not, by itself, justify continuous GPS tracking outside working hours; similarly, a duty to protect confidential information does not automatically permit unrestricted inspection of every communication.

6.3 Information technology and cybersecurity

Government departments may rely on applicable information-technology legislation,

¹²Digital Personal Data Protection Act 2023, Act 22 of 2023, s 1 and commencement notification GSR 843(E), Gazette of India, 13 November 2025.

¹³Digital Personal Data Protection Rules 2025, GSR 846(E), Gazette of India, 13 November 2025, r 1.

cybersecurity directions and internal security policies when monitoring networks or investigating threats. Such monitoring may be justified, particularly where it protects public records or sensitive systems. Cybersecurity should not, however, become a general rationale for unrelated profiling of employees. The collection of information and access to it should be confined to what is reasonably connected to the security objective and authorised by law.

6.4 Administrative fairness and disciplinary use

Where surveillance data is used in disciplinary proceedings or other decisions with significant consequences, the employee should receive the procedural protections required by the relevant rules and law. Digital records may be incomplete, inaccurate or misleading when separated from their context. The department should be able to explain how the record was produced, why it is considered reliable and how it supports the conclusion reached. Automated scores should not displace reasoned human judgment.

7. Technology-Specific Risks

7.1 Biometrics

Biometric attendance systems may be justified where identity fraud presents a demonstrated problem. However, biometric identifiers are difficult to replace if compromised. Departments should assess whether a less intrusive authentication method would be effective, whether raw biometric data needs to be retained, how templates will be secured and which officials may access them. Additional information should not be collected simply because the technology makes it possible.

7.2 GPS and geolocation

Location monitoring may be relevant to field inspections or official travel, but it should ordinarily be confined to the authorised task and period. Tracking during breaks, after working hours or through personal devices raises more serious privacy concerns and calls for a separate justification. Where verification of location is necessary, a check-in at defined points may provide a less intrusive alternative to continuous tracking.

7.3 Email, messaging and device logs

Technical records, such as authentication events and access attempts, usually involve a different degree of intrusion from examining the content of communications. A graduated approach is therefore preferable. Departments should begin with technical indicators and move

to content review only where it is necessary and legally authorised. Any review should be limited to relevant material, and the reasons for escalating to a more intrusive method should be documented. Advance notice should explain the applicable policy, but should not be treated as a blanket waiver of privacy.

7.4 CCTV and audio-visual monitoring

CCTV may be justified at public-facing counters, entrances, record rooms and restricted facilities. Its proportionality depends on placement, field of view, whether audio is recorded, retention periods and access arrangements. Cameras should not be installed in places where bodily privacy is reasonably expected, and recordings should not be retained indefinitely in the absence of a legitimate reason.

7.5 AI-based performance monitoring

Automated productivity systems can convert activity logs into scores or risk indicators. The principal concern is not automation alone, but the possibility that an opaque or inaccurate proxy will influence consequential employment decisions. A defensible system should make relevant indicators understandable, be tested for errors and discriminatory effects, allow correction of underlying data and preserve meaningful human review. The greater the potential consequences for an employee, the more robust the explanation and review should be.

8. International Standards and Comparative Lessons

Article 12 of the Universal Declaration of Human Rights protects against arbitrary interference with privacy and correspondence. Article 17 of the International Covenant on Civil and Political Rights prohibits unlawful or arbitrary interference with privacy, family, home or correspondence. These instruments provide relevant international context for assessing State monitoring, although their domestic effect must be considered alongside Indian constitutional law.¹⁴¹⁵

The Council of Europe's Recommendation CM/Rec (2015)5 addresses the processing of personal data in employment and offers a useful comparative reference for transparency, purpose limitation and safeguards. Read alongside Bărbulescu, it supports the view that workplace monitoring should be tied to a defined purpose and proportionate to it. An

¹⁴Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) art 12.

¹⁵International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17.

employee's use of workplace equipment should not, by itself, be treated as justification for unrestricted access.¹⁶

These international materials are persuasive rather than automatically binding in India. Their value lies in the practical criteria they offer for interpreting broader privacy commitments and informing domestic policy and judicial reasoning.

9. Proposed Constitutional Review Framework

This paper proposes an eight-stage framework for assessing digital surveillance of government servants. The framework is normative: it synthesises existing constitutional doctrine with comparative safeguards rather than presenting a test already adopted by the Supreme Court in this specific form.

Stage 1 — Characterise the interference. Identify the types and sensitivity of data collected, the frequency and duration of monitoring, whether records are aggregated, who receives them, how long they are retained and what employment consequences may follow.

Stage 2 — Establish legal authority. Identify the statute, rule or other legally sufficient authority relied upon and determine whether the monitoring measure falls within its scope.

Stage 3 — Specify the legitimate objective. State the concrete administrative or security concern the system is intended to address, rather than relying on general appeals to efficiency.

Stage 4 — Assess suitability. Explain how the technology is capable of advancing the stated objective and whether the information collected is relevant to that purpose.

Stage 5 — Assess necessity. Consider whether an equally effective but less intrusive alternative is reasonably available, and record the reasons for rejecting practical alternatives.

Stage 6 — Balance benefits and harms. Evaluate the effect on privacy and dignity, potential chilling effects, errors, discriminatory impacts, the scale and duration of monitoring and its likely consequences.

Stage 7 — Examine safeguards. Review notice, access controls, retention and security measures, independent oversight, human decision-making and the availability of remedies.

Stage 8 — Reassess over time. Revisit necessity and proportionality when the purpose, technology or use of the system changes, and at suitable intervals during continued operation.

The proposed framework extends constitutional review across the surveillance lifecycle, from procurement and implementation to access, retention, secondary use and reliance on records in disciplinary proceedings. It also allows the intensity of review to reflect the degree of intrusion.

¹⁶Council of Europe, Committee of Ministers, Recommendation CM/Rec (2015)5 on the processing of personal data in the context of employment (1 April 2015).

A limited attendance log may call for ordinary safeguards, whereas continuous location tracking or inspection of communications content should attract more demanding scrutiny.

10. Recommendations

10.1 Adopt a uniform baseline policy. Union and State departments should issue a baseline policy identifying permitted categories of monitoring, their legal basis and purpose, retention periods, access rules and complaint procedures. Departments responsible for sensitive functions may adopt additional safeguards suited to their particular risks.

10.2 Require documented privacy-impact and proportionality assessments. Before introducing high-impact monitoring, a department should record its purpose and legal basis, the alternatives considered, expected benefits, foreseeable risks and proposed safeguards. The assessment should be revisited whenever the system or its use changes materially.

10.3 Apply data minimisation and purpose limitation. Information should be collected only to the extent needed for the stated objective. Reusing monitoring data for an unrelated investigation or for performance profiling should require an appropriate legal basis and a fresh assessment of necessity and proportionality.

10.4 Restrict continuous and off-duty tracking. GPS and device monitoring should ordinarily be confined to authorised duties and working periods. Any exception should have legal authorisation, be narrowly tailored to the need and be documented.

10.5 Distinguish technical logging from inspection of content. Network security measures should begin with the least intrusive indicators that are effective for the purpose. Access to the content of communications should require a stronger justification, a defined scope and appropriate authorisation.

10.6 Establish retention and deletion schedules. Routine logs should be deleted or de-identified once their purpose has expired, subject to any lawful preservation obligation. Indefinite retention should not be the default position.

10.7 Provide independent review of intrusive systems. High-impact surveillance should be reviewed by an authority independent of the immediate supervisory chain. Periodic audits should examine access, error rates, discriminatory risks and compliance with the governing policy.

10.8 Preserve human review and the ability to contest decisions. An adverse employment decision should not rest solely on an unexplained automated score. Employees should be able to challenge inaccurate records and dispute material inferences in accordance with the applicable rules.

10.9 Protect complaints and whistleblowing. Employees who raise good-faith concerns about unlawful surveillance should not face retaliation. Serious complaints should be capable of referral to an independent review mechanism.

10.10 Align policy with the DPDP commencement schedule. Departments should prepare for the phased operation of the DPDP Act and Rules, verify the latest notifications and avoid treating provisions as operative before their commencement.

11. Limitations and Further Research

This is a doctrinal study and does not measure how widely surveillance systems are used across Union or State departments. Nor does it comprehensively survey all service rules, departmental circulars or procurement contracts, which vary between institutions and may affect the legality of a particular system. Further empirical work could examine government procurement documents, employee grievances, privacy-impact assessments and interviews with administrators and public servants. Comparative research could also explore how other jurisdictions regulate public-sector monitoring and algorithmic decisions about employment. These limitations define the scope of the analysis rather than undermine its doctrinal argument. The proposed framework is intended as a legal and policy model that can be tested against particular departmental practices and refined through empirical research.

12. Conclusion

Digital monitoring can serve legitimate public-administration objectives, including attendance verification, cybersecurity, protection of public resources and the investigation of misconduct. The State's role as employer does not, however, displace its constitutional obligations. Government servants remain individuals with fundamental rights, and workplace supervision should not be treated as permission for unrestricted observation.

The constitutional basis for this position lies in Articles 14, 19 and 21, particularly the recognition of privacy in Puttaswamy and the proportionality analysis developed in later cases. Data-protection legislation, service rules and cybersecurity requirements must also be considered carefully. This includes attention to the phased commencement of the Digital Personal Data Protection Act 2023 and the Rules 2025. Comparative decisions offer useful guidance on notice, scope, alternatives and safeguards, but do not substitute for analysis under Indian constitutional law.

The paper's principal contribution is a proposed framework tailored to workplace surveillance

that combines legality, legitimate purpose, suitability, necessity, balancing and safeguards across the data lifecycle. It distinguishes routine administrative logging from more intrusive technologies and calls for stronger justification as monitoring becomes continuous, sensitive or consequential. In doing so, it avoids both a categorical ban on monitoring and the assumption that public employment authorises surveillance without meaningful limits.

Surveillance can be constitutionally accountable where it is lawful, necessary, proportionate, transparent to the extent appropriate, securely managed and subject to meaningful review. Privacy protection need not weaken public administration. Rather, it may strengthen the State's legitimacy by ensuring that accountability is pursued through methods consistent with constitutional limits.

Table of Cases

Anuradha Bhasin v Union of India (2020) 3 SCC 637.

Bărbulescu v Romania (2017) 44 BHRC 1, App no 61496/08 (ECtHR, 5 September 2017).

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

K S Puttaswamy (Aadhaar-5J) v Union of India (2019) 1 SCC 1.

Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.

Table of Legislation and Instruments

Constitution of India.

Central Civil Services (Conduct) Rules 1964, where applicable.

Digital Personal Data Protection Act 2023.

Digital Personal Data Protection Rules 2025.

Information Technology Act 2000.

International Covenant on Civil and Political Rights 1966.

Universal Declaration of Human Rights 1948.

Bibliography

Books

Ajunwa I, The Quantified Worker: Law and Technology in the Modern Workplace (Cambridge University Press 2023).

Nissenbaum H, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).

Solove DJ, Understanding Privacy (Harvard University Press 2008).

International materials

Council of Europe, Committee of Ministers, Recommendation CM/Rec (2015)5 on the processing of personal data in the context of employment (1 April 2015).

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

Universal Declaration of Human Rights, GA Res 217 A(III) (10 December 1948).

Official and citation resources

Ministry of Electronics and Information Technology, notification GSR 843(E), Gazette of India (13 November 2025).

Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules 2025, notification GSR 846(E), Gazette of India (13 November 2025).

Oxford Law Faculty, The Oxford Standard for the Citation of Legal Authorities (OSCOLA), 5th edn (2025).

