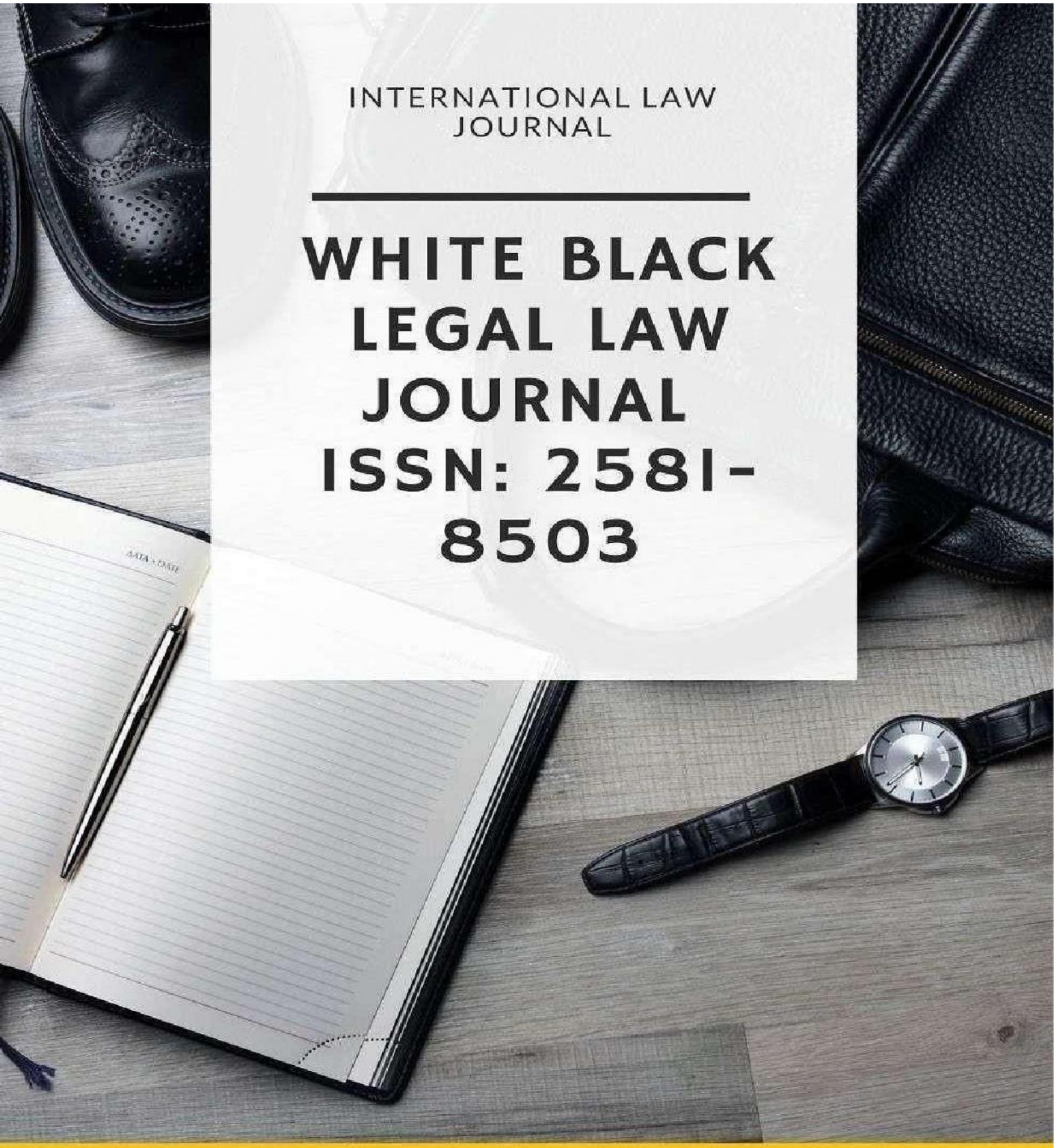


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

WHITE BLACK LEGAL

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

BIG BROTHER AT WORK: IS EMPLOYEE SURVEILLANCE COMPATIBLE WITH LABOUR RIGHTS?

AUTHORED BY - ATHITI B KANNAN
Institution: VIT School of Law, VIT Chennai

Abstract

Technology has changed the way people work and the way employers monitor their employees. Employers may use CCTV cameras, screen-recording software, keystroke tracking, biometric attendance systems, location tracking and artificial intelligence (AI) to supervise work. These methods can help protect confidential information and organise work, but they can also affect employee privacy, dignity and fairness. This paper examines whether digital workplace surveillance is compatible with employee rights under Indian law. It uses doctrinal legal research to analyse Article 21 of the Constitution, the Supreme Court's privacy jurisprudence, the Digital Personal Data Protection Act, 2023, relevant labour legislation and selected principles from the European Union's General Data Protection Regulation. The paper argues that the main issue is not whether employers should be allowed to monitor work, but whether monitoring is necessary, proportionate, transparent and used fairly. It proposes a practical framework based on purpose-specific monitoring, data minimisation, clear notice, limited retention, human review of consequential decisions and a meaningful process for employees to challenge inaccurate records. It also explains that the DPDP Act has a phased commencement schedule, meaning that its substantive provisions must not be treated as already operative merely because the Act has been enacted. The paper concludes that India should develop clearer workplace-surveillance standards that protect employees without preventing legitimate management and security measures.

Keywords: Workplace surveillance; employee privacy; labour law; artificial intelligence; data protection; proportionality; algorithmic management.

1. Introduction

Imagine working in an office where your employer can see how much time you spend on your computer, which websites you visit, how often you type and how long you remain inactive. In some workplaces, software can take screenshots, record attendance, track location or generate reports about an employee's productivity. The information collected may affect performance ratings, warnings, promotion or even termination.

Workplace supervision is not new. Employers have always needed to organise work, protect property and ensure that employees follow reasonable workplace rules. What has changed is the amount of information that technology can collect and the speed at which it can be analysed. Digital systems can make monitoring continuous rather than occasional. They may also produce scores or predictions that appear objective even when they do not fully reflect the nature of the work being done.

Employers may argue that monitoring is necessary to prevent data theft, protect confidential information, maintain safety and ensure that work is completed properly. Employees, however, have an interest in keeping personal information private and being treated with dignity. The concern becomes more serious when monitoring takes place without clear notice or when software-generated information is used without checking whether it is accurate.

This raises an important legal question: where should the law draw the line between an employer's legitimate interest in managing work and an employee's right to privacy and fair treatment? In India, the answer involves constitutional privacy principles, data-protection legislation, employment rules and the fairness of disciplinary procedures. These sources do not all apply in the same way, particularly where the employer is a private organisation.

This paper argues that workplace surveillance should be assessed through a proportionality-based framework. Employers should identify a legitimate purpose, choose a reasonably limited method of monitoring, explain the practice to employees and avoid relying entirely on automated assessments for serious employment decisions. The paper does not argue that all monitoring is unlawful. Instead, it examines when monitoring may become excessive or unfair and what safeguards should be introduced.

2. Research Problem

The main problem with digital workplace surveillance is that employers generally control the monitoring technology, the data it collects and the way the data is interpreted. Employees may not know exactly what information is recorded, how long it is stored, who can access it or whether it will be used for a purpose different from the one originally explained.

For example, an employee who spends time reading a long legal document, speaking to a client or thinking through a difficult problem may not produce continuous keyboard activity. A system that treats keyboard activity as a direct measure of productivity could therefore produce a misleading result. If that result is used to issue a warning or assess performance without further review, the employee may have little opportunity to correct the mistake.

The research problem is therefore whether the existing Indian legal framework provides sufficiently clear safeguards against excessive workplace monitoring and unfair decisions based on monitoring data. It also asks how employee privacy can be protected without preventing employers from taking reasonable steps to protect their business and manage work.

3. Objectives of the Research

- To explain the meaning and development of digital workplace surveillance.
- To examine the right to privacy under Indian constitutional law and its relevance to employment.
- To analyse the Digital Personal Data Protection Act, 2023, including its phased commencement, and relevant labour-law principles.
- To consider how AI-based monitoring can affect performance evaluation and disciplinary decisions.
- To compare selected Indian legal principles with safeguards under European data-protection law.
- To propose practical safeguards that balance employee rights with legitimate employer interests.

4. Research Questions

- To what extent should employers be allowed to monitor their employees?
- How do Indian privacy and data-protection principles apply to workplace surveillance,

particularly in private employment?

- Can monitoring data be treated as reliable evidence of employee performance or misconduct without further review?
- What safeguards should apply when AI-assisted assessments may affect an employee's livelihood?
- How can Indian law balance employer interests with employee privacy, dignity and procedural fairness?

5. Research Methodology and Scope

This paper follows a doctrinal method of legal research. It examines constitutional provisions, legislation, judicial decisions and selected comparative legal materials. The main Indian sources are Article 21 of the Constitution, the Supreme Court's decisions on privacy, the Digital Personal Data Protection Act, 2023, and the Industrial Relations Code, 2020 and Occupational Safety, Health and Working Conditions Code, 2020 where relevant. The paper also considers Article 22 of the European Union's General Data Protection Regulation as a comparative example.

The research does not use interviews, surveys or statistical data. It does not claim that all Indian employers use surveillance software or that every form of monitoring results in unfair treatment. Its focus is the legal framework and the safeguards that may be appropriate when employee information is collected or used to make decisions. Since statutory commencement dates can differ, the paper distinguishes between enactment of a law and the date on which particular provisions become operative.

WHITE BLACK LEGAL

6. Workplace Surveillance in the Modern World

- Workplace surveillance refers to methods used by employers to observe, record or analyse employee activities. Traditional methods included physical supervision, attendance registers and CCTV cameras. Digital systems now allow employers to collect more detailed information and combine it to form a picture of an employee's behaviour.
- Computer monitoring may include screenshots, website logs, application usage and keyboard activity.

- Location tracking may be used for employees who travel for work or perform duties outside the office.
- Biometric attendance systems may use fingerprints or facial recognition to record attendance.
- Productivity tracking may measure task completion, time spent on applications or periods of inactivity.
- AI-assisted monitoring may analyse collected data and generate scores, alerts or performance assessments.
- These methods are not equally intrusive. A camera at a building entrance for security purposes raises different concerns from software that records an employee's screen throughout the working day. Likewise, tracking a delivery worker's location while a delivery is being made may have a clearer connection to the work than tracking the same person outside working hours.
- The legal and ethical question should therefore not be answered by treating all monitoring as one category. The purpose, amount of information collected, timing, context, retention period and consequences for the employee should all be considered. Monitoring that is limited to a genuine security need may be easier to justify than continuous collection of information about every activity.

7. The Right to Privacy Under Indian Law

7.1 Article 21 and the recognition of privacy

Article 21 of the Constitution protects life and personal liberty. In Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-judge Bench of the Supreme Court recognised privacy as a fundamental right. The judgment connected privacy with dignity, autonomy and the ability of individuals to exercise control over important aspects of their lives. Privacy is not limited to secrecy; it can also concern the conditions under which information about a person is collected and used.

Although Puttaswamy did not directly decide a dispute about employee monitoring, its principles are relevant when considering the effects of surveillance on dignity and informational privacy. Location records, browsing history, biometric identifiers and screenshots may reveal information about an employee beyond whether a particular task has been completed.

However, Article 21 does not automatically make every monitoring practice by a private

employer a direct constitutional violation. Fundamental rights are generally enforceable against the State and other bodies that fall within the relevant constitutional rules, subject to specific exceptions and doctrines. A dispute between a private employer and an employee may therefore require consideration of statutory duties, employment terms, applicable service rules and other legal remedies, rather than assuming that Article 21 applies in exactly the same way as it does against the State.

This distinction is important. Puttaswamy provides a constitutional foundation for understanding why privacy matters, but it should not be cited as if the Supreme Court had already laid down a complete legal code for private workplace surveillance.

7.2 Proportionality and the balance of interests

Employers have legitimate interests in protecting confidential information, preventing fraud, ensuring safety and organising work. Employees also have an interest in privacy and in being assessed fairly. A useful way to examine the conflict is to ask whether the monitoring has a legitimate purpose, whether the method is connected to that purpose, whether a less intrusive method could reasonably achieve the same result and whether the benefit justifies the effect on employees.

For example, if an employer wants to prevent unauthorised access to confidential files, logging access to those files may be sufficient. Recording every keystroke or taking screenshots every few minutes may collect much more information than is needed. Similarly, monitoring attendance may be justified for a particular purpose, but it does not automatically follow that the same data should be used to assess commitment, productivity or promotion prospects.

A proportionality-based approach does not mean that employees can never be monitored. It means that the extent of monitoring should match the purpose for which it is used. It also requires attention to the context: a safety-sensitive workplace may have different monitoring needs from an office where the main tasks involve research, drafting or creative work.

8. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is an important part of India's developing data-protection framework. It creates a legal structure for the processing of digital personal data and sets out obligations for Data Fiduciaries and rights and duties connected with Data Principals. Employee information collected through digital attendance systems, monitoring software or location tracking may raise questions under this framework, depending

on the facts and the provisions in force.

Section 7(i) of the Act provides a specified legitimate-use ground for processing personal data for employment-related purposes and certain purposes connected with safeguarding an employer from loss or liability, including protection of trade secrets and confidential information. This provision should not be treated as an unlimited permission to collect any information about employees. The scope of a provision must be read with the Act as a whole and with the purpose and circumstances of the processing.

A crucial point for this paper is commencement. The Act received assent in 2023, but the Central Government's notification of 13 November 2025 provides for phased commencement of its provisions. The provisions listed in the later phase, including sections 3 to 17 and therefore the core processing framework relevant to sections 7 and 8, are scheduled to commence eighteen months after publication of the notification. As at 27 October 2026, those provisions should not be described as already in force. The commencement status must be checked again at the time of publication, especially if the paper is submitted after the scheduled commencement date.

This timing matters to the argument. It would be inaccurate to present the DPDP Act's substantive duties as fully operative in every respect at the time of writing. At the same time, the Act is relevant to the future legal framework and to the direction of Indian data-protection policy. A careful paper must distinguish between provisions already commenced and provisions that are enacted but scheduled to commence later.

WHITE BLACK LEGAL

Even once applicable, data-protection compliance alone may not answer every question about fairness in employment. A processing activity may have a legal basis while still raising questions about whether the monitoring is excessive, whether the data accurately reflects performance and whether a serious decision should be made without a meaningful opportunity for the employee to respond.

9. Artificial Intelligence and Unfair Employee Evaluations

AI-assisted systems can analyse employee activity and produce reports about attendance, task completion, response times or productivity. These systems may help managers identify

patterns, but their output depends on the information collected and the assumptions used by the software. A score may appear objective because it is numerical, even when it does not capture the full context of the work.

For example, a worker who spends several hours reading documents may produce fewer keyboard events than a worker performing repetitive data entry. An employee handling a complicated assignment may take longer than another employee performing a routine task. If the system focuses mainly on activity levels or speed, it may confuse visible computer activity with actual work quality.

There may also be risks if a monitoring system produces inaccurate data, uses a poor performance measure or treats different kinds of work as if they were identical. The paper does not claim that all AI systems are inaccurate. The point is that the reliability of a particular system should be examined before its output is used to make a consequential employment decision.

A serious warning, loss of pay, denial of promotion or termination should not be based only on an unexplained automated score. A fair process should allow the employee to understand the concern, correct factual errors and explain circumstances the system may not have considered. A manager should examine the evidence and give reasons for the final decision rather than treating the software's output as conclusive.

Indian law does not currently provide a single, universal and standalone right to human review of every AI-assisted employment decision. The availability of safeguards depends on the applicable legal framework, employment relationship and facts. This makes it useful to consider whether clearer standards should be introduced for decisions that have a serious effect on an employee's livelihood.

10. Can Employers Rely on Employee Consent?

Employers may argue that employees have agreed to monitoring by signing an employment contract or accepting a company policy. However, consent in an employment relationship can be complicated. Employees may feel that refusing a policy could affect their chances of obtaining or keeping a job. The existence of a signed document therefore does not, by itself, answer every question about fairness or the extent of monitoring.

An employer should explain what information is collected, why it is needed, how it will be used, who can access it and how long it will be retained. Employees should also be informed if information collected for security purposes may later be used for performance assessment or disciplinary action. A material change in monitoring should not be hidden in a general policy that employees are unlikely to understand.

The legal effect of consent must be assessed under the provisions applicable at the relevant time. In particular, the DPDP Act's commencement is phased, so its consent provisions should not be represented as fully operative before their notified commencement. The broader policy point remains that clear notice and meaningful explanation are important safeguards, even where an employer relies on another lawful basis for processing.

For example, if software records screenshots or tracks computer activity, employees should be told whether the purpose is information security, timekeeping or performance assessment. The employer should avoid collecting information unrelated to that purpose and should not use the data in a way that employees could not reasonably understand from the policy.

11. Workplace Surveillance and Labour Law

Workplace surveillance becomes especially important when collected information is used to take disciplinary action. The Industrial Relations Code, 2020 deals with matters including industrial relations, standing orders and dispute-resolution mechanisms. Its relevance to a particular monitoring dispute depends on the applicable provisions, the establishment, the category of employee and the circumstances of the action taken.

If digital records are relied on as evidence of misconduct, the employer should consider whether the records are accurate, complete and properly interpreted. For example, a system showing inactivity does not necessarily prove that an employee was not working. An employee may have been reading, attending a call or completing work away from the computer. A fair process should consider the explanation and the surrounding evidence before reaching a conclusion.

The Occupational Safety, Health and Working Conditions Code, 2020 may also be relevant where monitoring relates to safety or working conditions. However, neither Code should be

treated as a general authorisation for unlimited surveillance. Their provisions must be applied to the particular employment relationship and the issue in dispute.

Labour law is concerned not only with management's ability to organise work but also with the rules and processes that govern employment. Where monitoring data contributes to disciplinary action, the question should not be limited to whether the employer possessed the data. It should also include whether the data was reliable, whether the employee had a fair opportunity to respond and whether the decision was reached under the applicable rules.

12. A Comparison with European Law

The European Union's General Data Protection Regulation (GDPR) provides a useful comparative example. It includes principles of lawfulness, fairness and transparency, data minimisation, purpose limitation, storage limitation and accountability. These principles help explain why organisations should collect information for defined purposes and avoid keeping personal data for longer than necessary.

Article 22 of the GDPR addresses certain decisions based solely on automated processing that produce legal effects or similarly significant effects for an individual. It is not a complete ban on automated decision-making. It operates within specified conditions and exceptions and includes safeguards in the cases to which it applies, including rights relating to human intervention and contesting a decision.

The GDPR does not automatically apply to every Indian employer. Its territorial scope depends on the conditions in Article 3. It should therefore be used as a comparative model rather than treated as binding Indian law in every employment relationship.

The comparison is still useful because it shows how law can address risks created when automated systems make important decisions about people. India could consider more specific safeguards for high-impact employment decisions, including a clear explanation of the role played by monitoring data, a review by a responsible human decision-maker and an opportunity to challenge inaccurate information. Any such reform should be drafted with attention to Indian labour-law institutions and the phased operation of the DPDP framework.

13. A Proposed Framework for Fair Workplace Surveillance

The paper proposes a practical framework based on proportionality. The aim is not to prohibit legitimate supervision, but to ensure that monitoring is connected to a clear purpose and does not create avoidable harm to employees.

13.1 Clear workplace monitoring policies

Employers should maintain a written policy explaining the types of monitoring used, the purposes for which they are used, the categories of information collected, the persons who may access the information and the circumstances in which it may be shared or used for employment decisions. The policy should be written in clear language and provided before monitoring begins or when a significant change is introduced.

A policy should also explain whether monitoring is continuous or occasional, whether it applies outside normal working hours and how employees can ask questions or raise a complaint. A general statement that the employer may monitor all activity may not provide a useful explanation of what actually happens.

13.2 Necessity and proportionality

Before introducing a monitoring system, an employer should identify the specific problem it is trying to address and consider whether a less intrusive method could achieve the same result. If access logs can protect confidential files, continuous screenshots may not be necessary. If the purpose is attendance, the employer should consider whether collecting location or browsing data adds anything relevant.

The intensity of monitoring should also reflect the nature of the work. A safety-sensitive role may justify controls that would be excessive for a role involving research or drafting. Employers should review monitoring practices periodically to ensure that they remain necessary and do not continue simply because the technology is available.

13.3 Human review of consequential decisions

When monitoring data or an AI-generated report contributes to a serious employment decision, a responsible person should review the evidence before a final decision is made. The reviewer should consider whether the system is suitable for the task, whether the data is accurate and whether there are reasonable explanations for the result.

Employees should have an opportunity to understand the main reason for the concern and

correct relevant errors. The review should be meaningful rather than a formality in which a manager automatically accepts the software's conclusion. This safeguard is especially important where the decision could affect employment, pay, promotion or disciplinary status.

13.4 Purpose limitation, retention and security

Information collected for one purpose should not automatically be used for an unrelated purpose. For example, data collected to investigate a security incident should not routinely become a general measure of employee commitment without a clear and justified basis. Employers should set reasonable retention periods and restrict access to staff who need the information for their work.

Monitoring records should be protected against unauthorised access, alteration or disclosure. Once the information is no longer required for the stated purpose and no legal obligation requires retention, it should be deleted or otherwise handled in accordance with the applicable law and policy.

13.5 A meaningful complaint mechanism

Employees should have a clear way to question inaccurate records or raise concerns about monitoring. A complaint mechanism should identify the person or department responsible for receiving complaints, explain how the issue will be examined and provide a route for correcting errors. Where a decision was based on inaccurate data, the employer should reconsider the decision where appropriate.

This process would also benefit employers. A complaint may reveal a technical fault, a poorly designed productivity measure or a misunderstanding about the purpose of monitoring. Correcting the issue can improve both workplace trust and the quality of management decisions.

WHITE BLACK LEGAL

13.6 Specific guidance for AI-assisted employment decisions

India should consider issuing clearer guidance for the use of AI-assisted monitoring in employment. Such guidance could require employers to identify high-impact uses, assess whether the system is suitable for the task, explain the main factors used in an assessment and keep a record of human review for serious decisions.

The guidance should distinguish between low-impact tools, such as basic attendance records, and systems that rank employees or influence termination. A risk-based approach would allow employers to use ordinary management tools without unnecessary burdens while requiring

stronger safeguards where a mistake could seriously affect a person's livelihood.

14. Limitations of the Study

This paper is based on doctrinal legal research and does not include interviews, surveys or statistical information about workplace surveillance in India. It therefore does not measure how commonly particular monitoring technologies are used or how employees experience them in practice. The examples in the paper are illustrative and should not be read as findings about every employer.

The legal position is also affected by the phased commencement of the DPDP Act and Rules. The status of the relevant provisions should be rechecked immediately before publication. Further research could examine the experiences of employees in information technology, logistics, manufacturing, customer service and platform-based work. Empirical research could help establish which monitoring practices are most common and whether employees understand the policies that govern them.

15. Conclusion

Digital workplace surveillance has created new questions for employee privacy and labour rights. Employers can now collect and analyse information about employee activities on a much larger scale than was possible through traditional supervision. These tools may serve legitimate purposes, including protecting confidential information and ensuring safety, but they can also become excessive or produce misleading conclusions about performance.

WHITE BLACK LEGAL

Indian privacy jurisprudence provides an important foundation for understanding the connection between privacy, dignity and personal autonomy. However, constitutional rights do not automatically apply to every private employment dispute in the same way. Data-protection law and labour-law rules must also be examined carefully, and the commencement status of the DPDP Act must be stated accurately. Enactment and commencement are different legal stages.

The main concern is not surveillance by itself, but surveillance without adequate limits or accountability. A system that records activity without explaining its purpose, keeps data indefinitely or treats an automated score as conclusive can create an unfair imbalance between

employer and employee. This risk becomes more serious when the result affects a person's job or livelihood.

In my view, India should adopt a clearer proportionality-based approach to workplace surveillance. Employers should explain what they monitor and why, collect only information reasonably connected to that purpose, protect the data, limit retention and provide a way to challenge inaccurate records. Where monitoring data contributes to a serious employment decision, the decision should receive meaningful human review and should not depend entirely on a software-generated score.

The solution is not to prohibit workplace surveillance completely. It is to ensure that legitimate supervision does not become unlimited observation. As workplaces become increasingly digital, fair and transparent monitoring practices can help protect employee dignity while allowing employers to manage their organisations responsibly.

References

A. Legislation

- Constitution of India, arts 12 and 21.
- Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, 13 November 2025, read with the applicable commencement notification and any subsequent corrigendum.
- Industrial Relations Code, 2020 (Act No. 35 of 2020).
- Occupational Safety, Health and Working Conditions Code, 2020 (Act No. 37 of 2020).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), [2016] OJ L119/1.

B. Cases

- Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
- Maneka Gandhi v Union of India (1978) 1 SCC 248.

C. Official and Primary Sources

- Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025, Gazette notification, https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf (accessed 27 October 2026).
- Ministry of Electronics and Information Technology, Government of India, https://www.meity.gov.in/ (accessed 27 October 2026).
- Ministry of Labour and Employment, Government of India, https://labour.gov.in/ (accessed 27 October 2026).
- European Union, General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 27 October 2026).
- Justice K.S. Puttaswamy (Retd.) v Union of India, Indian Kanoon, https://indiankanoon.org/doc/91938676/ (accessed 27 October 2026).

WHITE BLACK LEGAL