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

VOLUME 5 AND ISSUE 12 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

WORK PLACE SURVEILLANCE AND DATA PROTECTION: THE NEW DIMENSION OF LABOUR RIGHTS IN CYBER SPACE

AUTHOR - ANBU RANI A* & S.GOWSALYA**

*LLM STUDENT AT CYBER SPACE LAW AND JUSTICE, THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY

**LLM STUDENT AT LABOUR LAW AND ADMINISTRATIVE LAW, THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY

BEST CITATION - ANBU RANI A & S.GOWSALYA, WORK PLACE SURVEILLANCE AND DATA PROTECTION: THE NEW DIMENSION OF LABOUR RIGHTS IN CYBER SPACE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (12) OF 2025, PG. 1037-1041, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract:

In the digital economy, the boundaries of the workplace have extended into cyber space, creating new challenges for labour regulation and employee rights. Employers in India increasingly deploy technologies such as CCTV, biometric attendance, email monitoring, and GPS tracking to monitor workers' productivity and ensure organisational security. However, these measures often conflict with the fundamental right to privacy, now constitutionally protected under Article 21. This paper explores how Indian labour rights intersect with data protection and workplace surveillance, analysing the constitutional foundation, statutory framework under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 (DPDP Act), and the relevant judicial pronouncements. It argues that the unchecked use of surveillance mechanisms risks undermining dignity, autonomy, and fairness in employment relations. The study concludes by proposing a balanced framework rooted in constitutional morality, employer accountability, and respect for informational privacy as a component of labour rights.

Key Words:

Workplace Surveillance, Data Protection, Right to Privacy, Labour Rights, Cyber Law.

INTRODUCTION:

The evolution of technology has transformed how employers interact with employees, reshaping the boundaries of work, control and privacy. In India, the proliferation of surveillance technologies- from **CCTV cameras in offices** to **keystroke loggers in remote work settings**- has triggered complex legal questions. While employers claim that such monitoring ensures productivity and data security, employees increasingly perceive it as intrusive and violative of their personal dignity.

The Indian legal system, rooted in constitutional guarantees, is now tasked with redefining labour protections in the digital era. This intersection **of cyber law and labour law** has become critical, especially after the recognition of the **right to privacy as a fundamental right** in Justice ***K.S. Puttaswamy (Retd) v. Union of India (2017).***[1773] The paper examines how constitutional values, statutory obligations, and judicial interpretations shape the contours of digital surveillance at workplace in India.

CONSTITUITONAL FOUNDATION: THE RIGHT TO PRIVACY:

The landmark judgment in ***Justice K.S. Puttaswamy (Retd) v. Union of India***[1774]

[1773] Justice K.S. Puttaswamy (Retd) and Anr. v. Union of India, (2017) 10 SCC 1.

[1774] Ibid.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

affirmed that privacy is intrinsic to the right to life and personal liberty under Article 21. The Supreme Court conceptualised privacy as encompassing physical, informational and decisional autonomy. This recognition marked a paradigm shift transforming privacy a mere common law right into a **constitutional entitlement**. Although the judgment primarily addressed state surveillance practices, particularly digital monitoring of employees communications or movements, engage constitutional values of dignity and autonomy.

In People's Union for ***Civil Liberties (PUCL) v. Union of India***[1775]**,** the court emphasised that telephone tapping constitutes a serious invasion of privacy and must adhere to strict procedural safeguards. By analogy, workplace surveillance through digital means should likewise satisfy the tests of legality, necessity, and proportionality laid down in *Puttaswamy*. Thus, Indian constitutional jurisprudence demands that any intrusion into privacy whether by the state or private employers must:

(a) Have a lawful basis;
(b) Pursue a legitimate aim; and
(c) Be proportionate and necessary.

LABOUR RIGHTS AND THE DIGITAL WORKPLACE:

The **right to dignity of labour** and **humane working conditions** under Article 42 of the Constitution and Directive Principles of State Policy gain renewed significance in cyberspace. Surveillance that treats workers as objects of algorithmic measurement undermines their dignity. Indian courts have long recognised that the right to livelihood under Article 21 includes fair and respectful treatment[1776]. With digital tools monitoring every movement of workers, the balance of power between employer and employee is further titled, calling for legal checks that align with constitutional morality.

STATUTORY FARMEWORK GOVERNING WORKPLACE SURVEILLANCE:

1. Information Technology Act, 2000:

The Information Technology Act, 2000 (IT Act) serves as the foundation for regulating electronic data and cyber activities. Section 43 A imposes liability on corporate entities for failure to protect sensitive personal data, while Section 72 A penalises unauthorised disclosure of information obtained under a lawful contract[1777].

Under the Information **Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,** employers were earlier required to obtained consent, inform data subjects about data usage, and maintain reasonable security practices[1778]. However, these rules were limited in scope and applied primarily to "body corporate."

Consequently, private employers had only general duties to protect employee data, leaving considerable discretion for monitoring and surveillance activities.

2. Digital Personal Data Protection Act, 2023:

The **Digital Personal Data Protection Act, 2023** (DPDP Act)[1779] marks India's first comprehensive data protection legislation. It introduces key principles such as lawful processing, purpose limitation, data minimisation, accuracy, retention limits, and reasonable security safeguards. Employers, as **"data fiduciaries,"** must process employee data for legitimate purposes and with transparency. The Act provides that personal data may be processed either on the basis of consent or for specific "legitimate uses."[1780]

However, reliance on consent in an employment relationship is problematic due to **unequal bargaining power** employees often

[1775] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[1776] Olga Tellis v. Bombay Municipal Corporation, AIR 1986 SC 180.
[1777] Section 72A, Information Technology Act, 2000.
[1778] Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[1779] The Digital Personal Data Protection Act, 203, Gazette of India, No. 18 of 2023.
[1780] Section 7, Digital Personal Data Protection Act, 2023.

cannot freely refuse consent without risking adverse consequences. Hence, employers should rely on legitimate is necessary and proportionate to the purpose.

The DPDP Act also confers **data principal rights**, including the right to access, correction, and grievance redress.[1781] Employers must appoint a **Data Protection Officer** (DPO) if classified as significant data fiduciaries.

By integrating these provisions into workplace practices, the Act extends **data protection obligations into employment spaces,** bridging cyber law with labour regulation.

JUDICIAL DEVELOPMENTS AND CASE ANALYSIS:

Indian jurisprudence on workplace surveillance remains nascent, yet several decisions illuminate the emerging contours of privacy in employment:

1. ***Justice K.S. Puttaswamy (Retd) v. Union of India (2017):*** established privacy as a constitutional right encompassing informational privacy.[1782]
2. ***People's Union for Civil Liberties (PUCL) v. Union of India (1997):*** declared unauthorised phone tapping unconstitutional, setting procedural standards for interception.[1783]
3. ***District Registrar and Collector v. Canara Bank (2005):*** recognised privacy of bank records and extended privacy protection to individuals vis-a-vis non-state actors.[1784]
4. ***K.S. Puttaswamy (Aadhar-5J) v. Union of India (2018):*** upheld proportionality as the standard for lawful data collection and retention.[1785]
5. ***Madras High Court, Registrar General v. State of Tamil Nadu (2020):*** prohibited installation of CCTV cameras in changing rooms and restrooms, citing violation of privacy and dignity.[1786]

These cases collectively affirm that surveillance state or private must be lawful, necessary and proportionate. They provide the constitutional foundation for evaluating employer monitoring practices.

CHALLENGES IN REGULATING WORKPLACE SURVEILLANCE:

1. **Absence of Specific Labour Law Provisions:**

Indian Labour laws such as the **Industrial disputes Act, 1947** and **Factories Act, 1948** were enacted long before the digital age and lack provisions addressing electronic surveillance or data privacy. Hence, employee's rights against invasive monitoring rely primarily on general privacy principles.

2. **Consent and Power Imbalance:**

The employer- employee relationship is inherently unequal. "Consent" obtained in employment contexts cannot always be considered voluntary.[1787] The DPDP Act's flexibility for legitimate use must be interpreted with safeguards to prevent abuse.

3. **Lack of Awareness and Enforcement:**

Most employees are unaware of their data rights, and enforcement mechanism remains weak. While the DPDP Act establishes a Data Protection Board, its effectiveness depends on clear regulations and employee-friendly complaint procedures.

4. **Technological Overreach:**

Modern monitoring systems AI analytics, productivity trackers, and GPS collect vast data, sometimes extending beyond work hours, eroding the **right to disconnect.**[1788] This leads to mental fatigue and privacy erosion.

[1781] Section 12, Ibid.
[1782] Justice K.S. Puttaswamy (Retd), supra note 1.
[1783] PUCL v. Union of India, supra note 3.
[1784] District registrar and Collector v. Canara bank, (2005) 1 SCC 496.
[1785] K.S. Puttaswamy (Aadhar-5J) v. Union of India, (2019) 1 SCC 1.
[1786] Registrar General, Madras high Court v. State of Tamil Nadu, (2020) SCC Online Mad 1172.
[1787] Vidushi Marda, "Consent and Power in Employment Surveillance, "Indian Journey of Law and technology, Vol. 15 (2022), P. 41.
[1788] Smriti Irani, "Digital Overreach and the Right to Disconnect," Economic and Political Weekly, Vol. 58, No. 7 (2023), P. 19.

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

VOLUME 5 AND ISSUE 12 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

THEORETICAL LINK: PRIVACY AS A LABOUR RIGHT:

Informational privacy emerged as an essential element of dignity in labour. Surveillance transforms workers into **"data subjects,"** exposing them to profiling, ranking and algorithmic control. Internationally, the ILO Convention No. 190 on violence and harassment at work emphasises protection of dignity and personal integrity, extending logically to digital environments.[1789]

Thus, the recognition of privacy as a component of labour welfare aligns with India's constitutional ethos and Directive Principles.

SUGGESTIONS AND RECOMMENDATIONS:

1. **Statutory Workplace Privacy Code:**

The Ministry of Labour and the **Data Protection Board** should jointly frame a **"Workplace Privacy and Surveillance Code"** redefining standards for notice, consent, retention and prohibited areas (e.g., restrooms, private spaces)

2. **Data Protection Officer for Employers:**

Mandatory appointment of DPOs in medium and large enterprises to ensure compliance and employee grievance redressal.

3. **Transparency Obligations:**

Employers must disclose surveillance methods, duration and data retention policies to employees through clear written notices.

4. **Purpose and Retention Limits:**

Data should only be collected for specific, legitimate business needs and erased once the purpose is fulfilled.

5. **Collective Consultation:**

Employee union's works councils should be consulted before introducing new surveillance systems, ensuring participatory governance.

6. **Judicial Oversight:**

Labour Courts and tribunals should develop jurisprudence on digital privacy and establish remedies for unlawful monitoring.

7. **Awareness Campaigns:**

Awareness programs should be initiated by labour departments to educate workers on their data rights.

8. **Recognition of "Right to Disconnect":**

Employees should have a statutory right to disengage from work related communications beyond working hours, ensuring mental well being.

CONCLUSION:

The integration of cyberspace into employment has blurred boundaries between profession and private life. In India, the Digital Personal Data Protection Act, 2023, read with Puttaswamy, forms the cornerstone of employee data rights. Yet, without explicit workplace regulations, surveillance risks becoming a tool of control rather than productivity.

Balancing legitimate employer interests with the employee's right to privacy requires a nuanced, constitutionally guided approach. Recognising informational privacy as a labour right will uphold the dignity of the Indian worker in the digital age, ensuring that technology serves humanity not the reverse.

BIBLIOGRAPHY:

- Basu, Subhajit, Cyber Law in India, Oxford University Press, 2021.
- Gopalkrishnan, K.S., Data Protection Law and Practice, Eastern Book Company, 2024.
- Narain, Arvind, "Privacy and the Employee in Digital India," NUJS Law Review, Vol. 15 (2023).
- Singh, Avani, "Labour Rights and Data Protection: Indian Perspective," Indian Journal of Labour Economics, Vol. 66 (2024).
- Upadhyay, D., "Algorithmic Management and labour regulation," NLSIU Law Review Vol. 35 (2023).

WEBLIOGRAPHY:

- Ministry of Electronics and Information technology, digital Personal Data

[1789] International Labour Organization, Convention No. 190 on Violence and Harassment at Work, 2019.

Protection Act, 2023- https://www.meity.gov.in

- Supreme Court of India- Judgments database: https://main.sci.gov.in
- International Labour Organisation – https://www.ilo.org
- Law School Policy Review, "Surveillance at Work: The Right Not to Be Monitored" (2025).