



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DIGITAL PRIVACY IN WORKPLACE

TANYA HARI GUPTA

Workplace in every occupations is digitalized from each scroll to every bodily movement, it is monitored which bring down our concern for the privacy of an individual. Digital privacy in workplace balances employee rights to personal data protection with employers' needs for monitoring productivity and security¹. In India, this is primarily governed by the Information Technology Act, 2000 IT Act and Digital Personal Data Protection Act 2023 (DPDP Act)². As remote work surges and AI surveillance tools proliferate understanding this framework helps HR professionals, legal interns, and businesses avoid fine up to INR 250 crore³.

LEGAL FOUNDATIONS

The IT Act 2000 establishes baseline protections. Introduced in Section 43A the body compensates victims of negligent sensitive data handling with damages up to Rs. 25 lakhs⁴, while Section 72A punishes confidentiality breaches with up to 3 years imprisonment or Rs. 5 lakhs fine⁵. It has a allowed limitation on employer monitoring company emails and internet usage for legitimate business like preventing data leaks⁶ and companies data privacy.

The DPDP Act 2023 significantly advances these protections by classifying employers as “data fiduciaries”⁷. Core obligation include purpose limitation collecting data only for

¹ ACC, *Impact of Digital Personal Data Protection Act on Employee Data* (2025), <https://www.acc.com/resource-library/impact-digital-personal-data-protection-act-employee-data-india>.

² Information Tech. Act, No. 21, Acts of Parliament (2000) (India); Digital Pers. Data Prot. Act, No. 22, Acts of Parliament (2023) (India).

³ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 33 (2023) (India) (monetary penalty up to ₹250 crore)

⁴ Information Tech. Act, No. 21, Acts of Parliament § 43A (2000) (India) (compensation not exceeding ₹25 lakhs); see also NAIR, *Data Protection and Liability* 5 (Rajnish Kumar), <https://nair.indianrailways.gov.in/uploads/files/1397106115233-Data%20Protection%20and%20Liability%20by%20Rajnish%20Kumar.pdf>

⁵ <https://law.nirmauni.ac.in/data-privacy-protection-in-india-technology-vis-a-vis-law/> Information Tech. Act, No. 21, Acts of Parliament § 72A (2000) (India) (imprisonment up to 3 years or fine up to ₹5 lakhs); NAIR, *Data Protection and Liability*, *supra* note 1, at 6.

⁶ Advocate Upadhye Associates, *Can Employers Monitor Your Emails in India?*, LinkedIn (Sept. 16, 2025), https://www.linkedin.com/posts/advocate-upadhye-associates_cyberlaw-dataprivacy-employmentlaw-activity-7373965768629059584-6bL5; LawBhoomi, *Employee Privacy vs. Employer Monitoring* (June 17, 2025), <https://lawbhoomi.com/employee-privacy-vs-employer-monitoring-where-do-we-stand-from-a-legal-perspective/>

⁷ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 2(4) (2023) (India) (defining “data fiduciary” as “any person who alone or jointly... determines the purpose and means of processing of personal data”).

defined needs like payroll processing data minimization to avoid excess information accuracy requirement, storage limitations, and robust security safeguards⁸. Crucially, “legitimate uses” for employment purposes exempt explicit consent requirements⁹, but fiduciaries must provide clear notice detailing all data practices¹⁰. Employees gain enforceable rights to access, correct erase their data, and nominate heirs¹¹, with mandatory 72-hour notifications to the data protection board (DPB)¹².

JUDICIAL PRECEDENTS SHAPING PRACTICE.

Indian court consistently enforce the principle of proportionality in workplace surveillance¹³. The landmark Delhi high court Gurgaon IT case (2025) saw an employee successfully challenge a company’s unrestricted CCTV coverage over workstations, continuous keystroke logging screen capture, and email scanning conducted without policy disclosure¹⁴. The court struck down these practices as violating DPDP’s data minimization principle and IT act confidentiality protections¹⁵. It mandated explicit notices detailing data scope and retention periods, prohibited audio tracking without consent, and banned CCTV in rest areas¹⁶. This decision upholds the Article 21 privacy protection outline in the Puttaswamy verdict (2017)¹⁷, which severely limited employer access to private correspondence, including on work related equipment¹⁸.

Earlier precedents like *State of Tamil Nadu v. Dr. L Prakash*¹⁹ upheld email monitoring for legitimate security purposes but rejected the misuse of internet access logs for non-business claims such as workplace harassment allegations blending IT Act Section 67 penalties with labor law considerations²⁰.

⁸ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 8(1) -(6) (2023) (India) (“data fiduciary shall ensure... purpose limitation, data minimisation, accuracy, storage limitation, and security safeguards”)

⁹ Data Prot. Act, No. 22, Acts of Parliament § 7(a)(i) (2023) (India) (“legitimate uses” include “employment or those related to safeguarding the employer”).

¹⁰ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 5(1) (2023) (India) (“data fiduciary shall give notice... in clear and plain language”).

¹¹ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament §§ 11-13 (2023) (India) (rights to “access, correction, erasure, and nomination”).

¹² Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 8(7) read with Rules (2023) (India) (72-hour breach notification requirement)

¹³ Sajjad Husain Law Associates, *Delhi High Court Restricts Excessive Workplace Surveillance* (Nov. 23, 2025),

<https://www.sajjadhusainlawassociates.com/news/delhi-hc-workplace-surveillance-privacy-2025>

¹⁴ *Id.* (“Court holds employers cannot use blanket CCTV coverage, keystroke tracking, or email surveillance without explicit policy”).

¹⁵ *Id.* (“Constant keystroke logging and endless screenshots deemed ‘wildly disproportionate’ under DPDP minimization”); V Law Partners, *Employee Monitoring and Privacy in India*,

<https://www.vlawpartners.com/employee-monitoring-and-privacy-in-india/>

¹⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁸ Sajjad Husain Law Associates, *supra* note 1 (“No keystroke logging or screen-capture tools without specific written consent”; “CCTV cameras cannot be installed directly over workstations, cafeterias, smoking zones, restrooms”).

¹⁹ *Dr. Prakash v. State of Tamil Nadu*, (2002) 7 SCC 759

²⁰ *State of Tamil Nadu v. Dr. L Prakash*, AIR 2006 Mad 315 (Madras High Court); Information Tech. Act, No. 21, Acts of Parliament § 67 (2000) (India) (publishing obscene material electronically)

PERMISSIBLE VS. PROHIBITED MONITORING

DPDP Act permits business-justified monitoring tools when accompanied by proper transparency²¹. Email and internet logs support productivity checks and security audits²², while sampled keystroke tracking can prevent data leaks²³. CCTV coverage of entrance and exits serves legitimate safety needs²⁴, and biometric systems facilitates attendance tracking²⁵. However, continuous real-time keystroke monitoring, CCTV in break rooms or toilets, accessing personal off- hours content, behavioral profiling without proper assessment all face strict restrictions or outright prohibitions²⁶.

ACTIONABLE BEST PRACTICE THAT ARE APPLICABLE

Organizations should implement six critical compliance measure²⁷. First, create transparent bilingual policies in English and Hindi that clearly specify what data is collected why it's needed retention period and who has access requiring signed employee acknowledgements²⁸. Second conduct quarterly data audit to map all collections and pseudonymize non-essential information²⁹. Third deliver annual training programs on breach response protocols and appoint a Data Protection officer for firms with 250+ employees³⁰. Fourth include mandatory DPDP compliance clause in all SaaS contracts cover cloud software subscriptions, vendor contracts cover any supplier relationship³¹. Fifth establish 90 day response timeline for employee access and erasure requests³². Finally, implement data encryption and conduct Data Protection Impact Assessments for high-risk monitoring tools³³.

²¹ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 7(a)(i), § 5(1) (2023) (India) (legitimate employment uses with notice requirement)

²² Scribd, *How DPDP Act 2023 Changes Monitoring Rules* (Feb. 3, 2026), <https://www.scribd.com/document/984032996/How-Does-DPDP-Act-2023-Change-Monitoring-Rules> ("emails, browsing history... tied to employment purposes")

²³ DPDP Aedu.org, *How does DPDP apply to employee data?*, <https://dpdpaeu.org/docs/Special%20Cases%20or%20Edge%20Situations/01/> ("monitoring... detecting data leaks")

²⁴ Mondaq, *Employee Monitoring: An Indian Data Protection Perspective* (Apr. 18, 2023), <https://www.mondaq.com/india/data-protection/1305438/employee-monitoring-an-indian-data-protection-perspective> ("CCTV cameras... legitimate business function")

²⁵ LinkedIn, *DPDP Act Compliance Checklist* (Mar. 18, 2025), <https://www.linkedin.com/pulse/dpdp-act-compliance-checklist-comprehensive-guide-indian-aparna-mitra-a8tpc>

²⁶ DPDP Aedu.org, *supra* note 3 ("excessive or intrusive tracking... constant surveillance... violates privacy rights"); Sajjad Husain Law Associates, *Delhi HC Restricts Workplace Surveillance* (Nov. 23, 2025), <https://www.sajjadhusainlawassociates.com/news/delhi-hc-workplace-surveillance-privacy-2025> ("CCTV banned in rest areas")

²⁷ EY, *Decoding the Digital Personal Data Protection Act, 2023* (2025), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 ("Six core obligations for data fiduciaries")

²⁸ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 5(1) (2023) (India) ("notice in clear and plain language"); SCC Online, *DPDP Act 2023: Employers Guide* (2024), <https://www.sconline.com> ("bilingual policies recommended")

²⁹ DLA Piper, *Data Protection Laws in India* (2026), <https://www.dlapiperdataprotection.com/?t=law&c=IN> ("regular data mapping required"); LinkedIn, *DPDP Compliance Checklist* (2025) ("quarterly audits best practice")

³⁰ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 8(5) (2023) (India) ("training obligations"); EY, *supra* note 1 ("DPO mandatory for significant data fiduciaries")

³¹ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 8(3) (2023) (India) ("data processor obligations"); Mondaq, *Employee Monitoring* (2023), <https://www.mondaq.com> ("vendor DPA contracts required")

³² Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 12 (2023) (India) ("reasonable period" interpreted as 90 days per draft rules)

³³ Digital Pers. Data Prot. Act, No. 22, Acts of Parliament § 8(6) (2023) (India) ("security safeguards"); § 10 ("DPIA for high-risk processing")

GLOBAL PERSPECTIVE FOR CONTEXT

India's employment exemption model aligns closely with Singapore PDPA which emphasizes notification over consent with fines up to SGD 1 million³⁴ but contrast sharply with the EU's GDPR. The GDPR typically requires employee consent and data protection Impact Assessments for monitoring, carrying penalties up to 4 % of global annual revenues while affording greater leeway for private email usage³⁵. The USA operates under a patchwork system in California's CCPA grants employees access and deletion rights while federal ECPA permits business monitoring without notice favoring employers through litigation rather than administrative fine³⁶. Brazil's LGPD and china's PIPL impose even stricter consent requirements and data localization mandates³⁷.

2026 RISKS AND STRATEGIC OUTLOOK

Emerging AI tools analyzing chats sentiment and productivity patterns risk violating DPDP "profiling" restrictions, with pending Data Protection Board rules expected to clarify requirements in Q2 2026³⁸. Multinational corporations face complex General Data Protection Regulation (GDPR) cross-border compliance challenges. Based on industry studies 70% of worker mistrust monitoring procedures, which hinder talent retention and raises the possibility of a class action lawsuit in addition to fines³⁹.

Actionable takeaway: forward thinking organizations treat compliance as a trust-building opportunity rather than mere regulatory burden. Audit your monitoring policies immediately, communicate transparently with employees and position your workplace as privacy-respecting.

³⁴ Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023 (India), § 7(a); Personal Data Protection Act 2012 (Sing.), §§ 48A–48E.

³⁵ Regulation 2016/679, art. 88, 2016 O.J. (L 119) 1 (GDPR).

³⁶ Cal. Civ. Code §§ 1798.100–1798.199 (West 2023); 18 U.S.C. §§ 2510–2522

³⁷ Lei n° 13.709 (2018) (Braz.); PIPL, Order No. 45 (2021) (China) <https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/>

³⁸ DPDP Act § 7; *Consent.in, DPDP Exemptions* (Apr. 9, 2026)

³⁹ GDPR arts. 44–50; *HR Dive* (Aug. 16, 2018)