Privacy by Design for Employers: An Indian Perspective

KPrashant Singh[*1], **Suman Madan**[2*]

[1] Research Scholar, Ugdx School of Technology, ATLAS SkillTech University, Mumbai, India
[1]KPrashant.singh0103@gmail.com
[2] Professor, Ugdx School of Technology, ATLAS SkillTech University, Mumbai, India
[2]Madan.Suman@gmail.com

Abstract The growing employee digital surveillance and data-driven human resource management has resulted in an imbalance between the privacy of an employee and organizational effectiveness. This paper examines how Indian firms can proactively incorporate privacy protections into their workplace systems and decision-making procedures by embedding Privacy by Design (PbD) as a framework. The study places privacy in the Indian organizational and sociocultural context by referencing the country's new data protection law, the Digital Personal Data Protection (DPDP) Act, 2023.

The purpose of this paper is to explore the behavioural phenomenon known as the employee privacy paradox, which refers to the discrepancy between employees' stated privacy concerns and their actual willingness to share personal data in the workplace. Thus, this paper explores how employee attitudes and behaviours are shaped by willingness to disclose (WTD) and perceived data sensitivity (PDS), especially toward data collection methods such as biometric attendance, workplace surveillance, remote monitoring and AI-based performance analytics.

This paper further emphasizes how misalignments between employee perceptions and employer practices can erode trust, reduce engagement, and heighten legal as well as reputational risks. It argues that effective implementation of PbD requires a distinct understanding of both PDS and WTD to ensure compliance with the law along with the commitment to ethical data stewardship.

The paper contributes to contextualizing PbD in Indian workplaces through the PDS–WTD framework.

Keywords: Employee Privacy Perceptions, Perceived Data Sensitivity, Employee Attitudes and Behaviours, Willingness to Disclose.

1 Introduction

The idea of privacy has developed as a fundamental right for employees across organizations. With increasing digitalization and the use of surveillance mechanisms such as biometric attendance and cloud-based data storage systems to manage employee data, the relationship between workplace efficiency and employees' privacy expectations has become more complex. Several studies exist that had examined the technical aspects of privacy preservation models in big data context [1,2], but the employee-centric behavioural aspect remains unexplored in India.

With the changing legal framework for privacy in India, the introduction of the DPDP Act, 2023, the privacy-by-design frameworks provide a proactive way to foster trust in managing data throughout the employee lifecycle[3]. The DPDP Act, India's first-ever comprehensive data protection law, includes key provisions relevant to employees that organizations must comply with, such as-

- Consent-based data processing – with specific expectations, considerable changes to existing employee contracts
- Transparency and purpose limitation to be incorporated in employee processes with specific notices
- Employers with have to deploy design measures and controls ensuring data minimization and accuracy obligations
- Employees (data principles in this case) will have rights to access, correction and deletion of data
- Ensuring compliance with reporting data breaches and deploying necessary security safeguards

The above measures must also be read in conjunction with existing legislation in similar domain such as Information Technology (Reasonable Security Practices and Procedures) Rules, 2011 under the IT Act, 2000; Indian Contract Act, 1872 (through confidentiality clauses) & Labour laws such as the Industrial Disputes Act, which may indirectly intersect with privacy during disciplinary proceedings or surveillance.

Countries such as Canada and EU members have long integrated Privacy by Design (PbD) principles into their employment frameworks[4]. Even so, Indian multinational companies, especially in IT/ITES sectors, are already implementing GDPR-aligned policies, offering templates for different domestic organizations. Privacy by design provides a proactive and future-proof framework for addressing employee data concerns by embedding privacy into organizational policies, processes, and technology systems from the outset. However, research on employee privacy in India remains limited. Existing studies predominantly reflect western contexts, where workplace dynamics, cultural norms, and legal frameworks differ significantly. The Indian scenario presents unique challenges, such as low privacy literacy, socio-economic variations, normalization of surveillance, and hierarchical workplace structures that discourage questioning data practices.

V. Agarwal et al. (eds.), *Proceedings of the Global Innovation and Technology Summit "AAROHAN 3.0"_HSS Track (GITS-HSS 2025)*, Advances in Social Science, Education and Humanities Research 1005,
https://doi.org/10.2991/978-2-38476-559-1_39

The objective of this paper is to address this gap by examining how PbD can be operationalized in Indian workplaces under the DPDP Act, with a particular focus on the behavioural phenomenon of the employee privacy paradox.

2 Privacy by Design – the theoretical framework and Contextual Employee Behaviour

PbD is an approach where privacy measures are integrated into the organizational business processes, technology controls and policies from the start, rather than being added later as compliance requirements. It focuses on deploying privacy-related measures into the employee process architecture and associated technology systems directly.

Fig. 1 shows the seven foundational principles of privacy by design which are widely acknowledged and form the basis of many privacy regulations such as the EU's GDPR and several emerging data protection laws worldwide. -

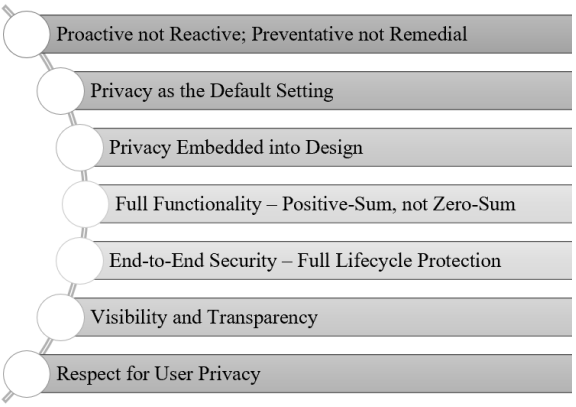

Fig 1: Foundational Principles of Privacy by Design

These principles provide a strategic framework for employers to address employee data concerns. As India transitions into a regulated data economy under the DPDP Act, embedding PbD into employment practices is not only a compliance necessity but also a crucial trust-building measure.

2.1 Application of Privacy by Design in employee context

PbD frameworks and technological measures can be applied across the entire data lifecycle of an employee, from recruitment to exit [5]. The following subsections illustrate how PbD principles translate into practice in the Indian workplace.

i. **Recruitment & On-boarding Stage:** The recruitment phase involves attracting, evaluating, and hiring the right talent for a role while the on-boarding stage concentrates on mixing new employees into the organization through orientation, training, and support for smooth adjustment. Measures suggested under Privacy by Design framework includes:

- Minimal data collection: Collect only necessary & job relevant data (e.g., education, work history)
- Use secure Third-party platforms for job applications/ background verification: Ensure compliance by background verification and recruitment portals, avoid intrusive background checks unless legally required
- Provide privacy notices upfront: Inform applicants about data usage and retention policies

ii. **Employment Lifecycle:** The Employee Lifecycle covers the phases of an employee's journey starting from recruitment, onboarding, development, and retention to exit. Measures suggested under Privacy by Design framework includes:

- Access controls: Implement role-based access to sensitive employee data
- Monitoring policies: Develop clear guidelines on surveillance (e.g., email, CCTV), Avoid excessive surveillance (e.g., keystroke logging, webcam monitoring) unless necessary and disclosed
- Employee consent: Obtain meaningful and non-coerced consent where required and maintain records of consent and notices

iii. **Offboarding:** Offboarding is the structured process of managing an employee's exit through knowledge transfer, clearance, and formal separation. Measures suggested under Privacy by Design framework includes:

- Data retention policies: Ensure secure deletion or archival of data as per retention policies
- Revocation of access: Disable access to internal systems immediately upon exit
- Right to erasure: Offer data erasure option unless retained for legal reasons

iv. **Workplace Surveillance:** Workplace surveillance is the monitoring of employee activities, communications, and performance using tools like CCTV, emails, or digital tracking. It seeks to balance security and productivity while addressing concerns about privacy and trust. Measures suggested under Privacy by Design framework includes:

- Justify CCTV monitoring, biometric systems, and productivity tracking tools under legitimate interest
- Clearly communicate the scope and purpose
- Avoid monitoring in private spaces (e.g., digital agents, break areas)

2.2 Integrating PbD with employee behaviour

Perceived data sensitivity suggests how sensitive an employee believes a certain type of data is in a particular workplace setting, while willingness to disclose is a measure of an employee's intent to reveal his/her personal information based on perceived trust on the purpose and data gathering process, cultural norms, and contextual relevance to point/purpose of data collection. Specific to India, disclosure behaviour is influenced by different factors such as cultural respect for authority, limited awareness of own's data rights, socio-economic disparities, and the widespread acceptance of deployed organizational surveillance practices such as biometric attendance and agent-based location tracking [6].

These elements contribute to the phenomenon known as employee privacy paradox, where employees voice concerns about their respective privacy concerns still they end up sharing personal information, especially when they perceive no alternative. This paradox deepens when workplace systems and processes lack clear controls & transparency especially handling employee sensitive data. The relationship of PDS and WTD is illustrated in Table 1. This interrelationship between data sensitivity and willingness to disclose significantly influences the implementation of privacy by design. Employers must tailor privacy processes and controls based on the type of data and employees' disclosure patterns. Sensitive data, such as health or financial information, requires robust safeguards, explicit consent, and transparent communication on purpose, usage and storage, whereas less sensitive professional data can be managed with less stringent measures. Some of the key privacy by design strategies like customized privacy notices, context-specific consent mechanisms, and employee training, help address these behavioural anomalies.

Table 1. Relationship between PDS, WTD and the Privacy Paradox

Data Sensitivity (PDS)	Willingness to Disclose (WTD)	Likely Behaviour	Privacy Paradox Effect
High (e.g., health, financial)	Low	Refusal or hesitation unless safeguards exist	Strong paradox when disclosure forced
High	High	Reluctant disclosure due to job pressure	Paradox visible, trust erosion
Low (e.g., job title, skills)	High	Easy disclosure	Minimal paradox
Low	Low	Limited disclosure, often comfortable	Negligible paradox

As discussed above privacy by design deployment at workplace extends beyond a technical or legal framework and encompasses a socio-behavioural dimensions. Its effectiveness is based on respecting employee perceptions, reducing unnecessary data collection, and embedding trust in design decisions. By deploying such practices, employers can achieve a balance between regulatory compliance and employee autonomy, meeting both organizational and individual expectations in the Indian workplace. To further refine the behavioural insights, Table 2 shows the effects of PDS and WTD implementation

Table 2: Effect of PDS and WTD on Privacy by Design Implementations

Factor	Employee Perspective	Implication for Privacy by Design (PbD)
Perceived Data Sensitivity	"Some data feels too personal to share (e.g., health, emotions)."	PbD should classify and tier data sensitivity, applying stronger safeguards to high-risk data.
Willingness to Disclose	"I'll share if I trust the system and have control."	PbD must support granular control, customized consent, and opt-in defaults.
Context & Culture Sensitivity	"Not all roles or cultures view data the same way."	PbD should enable context-aware configurations tailored to job role or location.

Transparency	"I want to know what's being collected and why."	PbD should provide **clear notices**, **data usage dashboards**, and **feedback loops**.
Trust Building	"I'll share if I believe my data won't be misused."	PbD should include **audit trails**, **explainable policies**, and **privacy seals**.
Data Minimization	"Don't ask for more than what's necessary."	PbD should follow the **data minimization** principle—**collect only what's essential**.

3 Literature Review

Employee privacy has become a pressing issue as organizations increasingly rely on digital monitoring and surveillance tools [7,8]. The adoption of PbD offers promise, but its application varies widely between India and Western nations due to differences in law and workplace culture. Studies show that two factors, namely perceived data sensitivity (PDS) and willingness to disclose (WTD), strongly influence employee privacy concerns [9,10]. At the core of employee privacy are two aspects: resisting invasive monitoring and maintaining control over personal information [11,12]. While employees value privacy, organizational demands often clash with these boundaries. Reviews across disciplines highlight how digital technologies have intensified concerns by making data collection more frequent and complex.

PbD takes a proactive stance by embedding privacy into systems and practices from the outset [13]. When sensitive data such as health records or biometric identifiers is involved, employees' willingness to share decreases, directly affecting trust and privacy management [14,15].

In India, socio-cultural realities such as hierarchical workplace structures and limited awareness of legal rights, further shape these concerns. Many employees fear misuse or see legal protections as weak [16,17]. Thus, effective PbD implementation requires integrating privacy into technology, company culture, policies and regulations [18]. Yet Indian employers still face challenges like weak enforcement, legal loopholes, and low awareness of data protection. Table 3 summarises the factors affecting perceived data sensitivity in the employee privacy context.

Table 3: Factors affecting perceived data sensitivity for an employee

Factor	Description	Key Findings	Reference
Type of Data	Different categories of data (e.g., personal, health, financial, biometric) vary in sensitivity.	Health and biometric data are consistently rated as more sensitive than work-related or contact data.	[7, 9-11]
Context of Collection	Sensitivity depends on where, why, and how data is collected in the workplace.	Data collected covertly or without clear purpose is perceived as more sensitive and intrusive.	[7-8, 12, 16]
Perceived Control	Employees' control over data use affects sensitivity perception.	Lack of control or ability to limit data access increases perceived sensitivity and concern.	[8,11-12,16]
Potential Harm	Risk of misuse, discrimination, or reputational damage increases perceived sensitivity.	Data likely to cause harm if disclosed (e.g., medical history) is deemed highly sensitive.	[7,12,16]
Cultural and Organizational Norms	Workplace culture and societal norms shape sensitivity levels.	Collectivist cultures may exhibit different sensitivity patterns; organizational norms moderate expectations.	[7-8,16,19]
Trust in Employer	The degree of trust employees have in their organization influences sensitive judgments.	Higher trust correlates with lower perceived sensitivity; distrust elevates concerns.	[11-12,16,20]
Legal and Policy Awareness	Awareness of privacy laws and internal policies impacts perceived data sensitivity.	Employees unfamiliar with protections perceive higher sensitivity due to uncertainty.	[7,16-17,21]
Disclosure Willingness	Sensitivity inversely affects willingness to disclose personal information.	More sensitive data leads to a reduced willingness to disclose, which in turn affects organizational data collection.	[9-10,15]

The reviewed literature highlights that while Privacy by Design has gained prominence globally, its application in India is still at a formative stage. Research consistently shows that perceived data sensitivity and willingness to disclose shape employee attitudes, yet empirical evidence on how these factors translate into workplace practices in India remains limited. This gap underscores the need for contextual frameworks that integrate behavioural insights with legal and organizational realities.

The next section addresses this need by presenting findings from recent industry studies and case examples, and by proposing a framework for Indian employers to operationalize Privacy by Design in employee data management.

4 Findings and Proposed Framework

Our study emphasizes how perceived sensitivity varies by data type or context and thus influences disclosure decisions. The privacy calculus theory explains that employees weigh perceived benefits against privacy risks while deciding whether to share personal data or not. The following are categorized findings based on our study regarding employee behaviour along with contextual parameters related to Indian workplaces that can be critical while implementing privacy by design.

i. **Empirical Findings in Workplace Privacy**

- Employees are more likely to be more protective of sensitive data like health, financial etc. However, in contrast, they are more willing to disclose professional details.
- Willingness to disclose information is designed by trust in employer, perceived fairness and norms around surveillance.
- The privacy paradox shows that some employees reveal despite of concerns because of the pressure of organizational or job security.

ii. **Indian Socio-Cultural Context:** Adoption of PbD in Indian workplaces is complicated by several factors:

- Limited awareness of data privacy rights
- Cultural morals that value hierarchy and deference may potentially reduce employees' resistance to data collection
- Minimal objection to biometric attendance and workplace monitoring.
- Women, lower-income workers and workers less digitally literate are more vulnerable since they often lack the power to resist intrusive practices.

iii. **Industry Studies and Reports:** Table 4 highlights gaps in privacy practices among Indian firms:

Table 4 Privacy Gaps & Future course

Publication/ Study	Findings	Future Suggestions
Cisco Cybersecurity Readiness Index 2025 (India Focus) [22]	• Only 10% of Indian firms are "Mature" in identity security; identity remains a top challenge. • Unmanaged devices & hybrid work expose sensitive employee/customer data. • Cloud readiness low (7%), leaving HR and employee data vulnerable. • AI adoption high, but shadow AI use (employees inputting HR/client data into GenAI tools) is a major risk. • Budget pressure: privacy budgets risk shrinking as AI governance gets priority.	• Adopt Zero Trust for identities, devices, and networks. • Strengthen cloud privacy safeguards (encryption, segmentation, unified policies). • Create GenAI governance frameworks restricting sensitive data use. • Balance budgets: ring-fence privacy funding even while investing in AI. • Increase employee privacy awareness training on rights & risks.
Cisco Privacy Benchmark Study 2025 [23]	• Trust paradox: 91% trust global providers more, yet 90% prefer local storage. • DPDPA positive impact (94% firms), but low awareness: only 26% of consumers/employees know their rights. • GenAI risk: 46% of firms input employee data, 31% input customer data into GenAI tools. • Privacy budgets under strain → shifting to AI governance. • Localization costs high, especially for SMEs.	• Launch awareness campaigns on DPDPA rights for employees and consumers. • Enforce GenAI data governance (masking, anonymization, audit trails). • Ensure balanced budget allocation between privacy and AI. • Strengthen vendor due diligence for cross-border and cloud providers. • Promote privacy-by-design AI frameworks to align with DPDPA
NASSCOM–DSCI–KPMG Study on Employee Privacy in IT/ITES [24]	• Only 24% had dedicated employee privacy policies, most bundled privacy under security. • Employee safeguards limited to NDAs and background checks, not rights. • Privacy officers rare; roles often merged with CISOs. • Training shallow – limited to induction, no structured awareness. • Culture compliance-driven (client data focus), not rights-driven. • Preference for self-regulation over legislation (83% firms)	• Draft dedicated employee privacy policies under DPDPA. • Assign Data Protection Officers (DPOs) with accountability. • Define retention limits for ex-employee data; enforce erasure rights. • Educate employees about consent, correction, and grievance mechanisms. • Regulate employee monitoring & surveillance with transparency and proportionality.

		• Move from self-regulation to compliance with DPDPA obligations.

Considering distinct gaps in understanding and addressing workplace privacy concerns in India, especially when factoring in socio-cultural dynamics, below are the key implications for policy & design -

- Need for contextual employee education on privacy.
- Design of culturally sensitive, low-literacy-friendly consent mechanisms.
- Inclusion of gender, caste, and class dimensions in privacy assessments.
- Development of employee co-created privacy frameworks in Indian organizations

Basis above discussion at a conceptual model, factors affecting (PbD) Privacy by design in workplace surveillance are summarised in table 5. These factors can act as a baseline measure for organizations while developing contours of data privacy programs for respective organizations. This shall not only provide organizations implementation awareness but also provide measures to be considered for addressing privacy by design as a concept – involving redesigning the business processes and implementing technical controls, ensuring compliance to the regulations.

Table 5 Factors affecting (PbD) Privacy by design in workplace surveillance

Factor	Description	Key Insight
Trust as a Foundational Determinant	Trust is the central enabler of privacy acceptance. Employees are more likely to accept surveillance if they trust their employer's motives, data use practices, and commitment to ethical behaviour. Organizational culture, leadership transparency, and prior experiences with monitoring shape trust levels. A lack of trust undermines even well-designed privacy frameworks	Without trust, even transparent or technically secure surveillance systems are perceived as invasive
Transparency and Communication	Transparency transforms surveillance from a covert operation into a negotiated practice. Employees must understand what data is collected, why, how it is used, and by whom. This clarity fosters informed consent and reinforces organizational accountability. However, token transparency—where policies are buried in complex legal terms—erodes credibility	Transparency must be continuous, clear, and dialogic—not a one-time legal disclosure
Employee Control and Informed Consent	Empowering employees with control over their data—such as opting in/out, customizing privacy settings, or limiting data sharing—strengthens PbD. Measures ensuing informed consent and control mechanisms respecting autonomy of an individual.	PbD is compromised when consent is symbolic rather than substantive
Data Sensitivity and Contextual Integrity	The nature of data collected, and the context critically affect privacy perceptions. Ensuring heightened safeguards for highly sensitive data.	A one-size-fits-all surveillance model fails to account for contextual nuances of privacy expectations
Legal and Ethical Compliance	Legal regulations like GDPR, CCPA, or national labour laws create the external scaffolding for privacy design. However, compliance alone is not sufficient, ethical principles (fairness, autonomy, non-maleficence) are required to address grey areas where law lags technology.	Ethical design extends beyond legal minimums to uphold moral responsibilities
Technological Implementation of PbD	Privacy must be embedded at the system design level which includes practices like data minimization, purpose limitation, anonymization, and encryption.	PbD is only as effective as the technical architecture and engineering practices behind it
Psychological and Social Considerations	Employee attitudes toward privacy are shaped by individual values, workplace norms, and cultural expectations. Some employees may view surveillance as protective, others as oppressive. The perception of fairness, dignity, and reciprocity influences whether surveillance is seen as a benefit or a threat	Privacy interventions must account for human behaviour, not just system design.
Organizational Policies and Monitoring Practices	The design and application of surveillance policies must be proportional, consistent, and purpose driven.	Fair, transparent enforcement builds legitimacy and minimizes privacy backlash.

5 Conclusion

Powered by emerging digital technologies and data-driven management, workplace surveillance is increasingly common especially post covid and advent new working environments. On one hand the deployment of such measures can improve efficiency, safety, and compliance but it raises significant employee privacy concerns as well. Implementing privacy by design (PbD) principles is critical to balancing these competing interests.

It is a complicated, socio-technical problem to implement the Privacy by Design paradigm in contemporary workplace contexts; there is no one-size-fits-all answer. In the workplace, factors such as trust in the purpose, process transparency, employee control, data sensitivity measures, legal-ethical alignment, technical robustness, psychological insights, and policy integrity interact dynamically to determine the success of PbD initiatives. A comprehensive, employee-centred strategy that places equal emphasis on data protection and dignity is necessary for sustainable workplace privacy.

The lack of sector-specific data protection standards, low privacy literacy, different levels of technical maturity, and cultural acceptance of surveillance practices (such as biometric attendance and agent-based laptop tracking) are some of the issues facing India. Adopting PbD presents both opportunities and challenges in the Indian job context. Although the DPDP Act has a strong legal basis, employees' desire to disclose and perceived data sensitivity must be addressed for effective implementation. Employers need to implement contextual, considerate, and inclusive privacy practices in order to move beyond just compliance. This strategy not only lowers legal risks but also improves corporate ethics and employee trust.

Privacy by Design is therefore a business requirement rather than just a regulatory requirement. Employers in India who incorporate privacy into their procedures and culture will increase employee trust, reduce legal risks, and get ready for the rapidly changing digital market.

References

1. Madan S, Goswami P (2021) A technique for securing big data using k-anonymization with a hybrid optimization algorithm. Int J Oper Res Inf Syst (IJORIS) 12(4):1–21. https://doi.org/10.4018/IJORIS.20211001.oa3
2. Chaudhury S, Dhabliya D, Madan S, Chakrabarti S. Blockchain Technology: A Global Provider of Digital Technology and Services. In: Building Secure Business Models Through Blockchain Technology: Tactics, Methods, Limitations, and Performance. IGI Global. 2023;p. 168–193. https://doi.org/10.4018/978-1-6684-7808-0.ch010
3. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/
4. https://www.millerthomson.com/en/insights/cybersecurity/made-in-canada-what-is-happening-to-privacy-by-design-under-the-cppa/
5. Anna Romanou,(2018)The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise, Computer Law & Security Review, Volume 34, Issue 1, Pages 99-110, https://doi.org/10.1016/j.clsr.2017.05.021.
6. Bu, F., Wang, N., Jiang, Q., & Tian, X. (2024). Research on Privacy-by-Design Behavioural Decision-Making of Information Engineers Considering Perceived Work Risk. Systems, 12(7), 250. https://doi.org/10.3390/systems12070250
7. M Dimodugno et al 2021, The effect of privacy concerns, risk, control, and trust on individuals decisions to share personal information: A game theory-based approach, J. Phys.: Conf. Ser. Vol. 2090 012017; DOI 10.1088/1742-6596/2090/1/012017
8. Kim, Y., Kim, S. H., Peterson, R. A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. Technological Forecasting and Social Change, 196, 122789
9. Tolsdorf, J., Reinhardt, D., & Lo Iacono, L. (2022). Employees privacy perceptions: exploring the dimensionality and antecedents of personal data sensitivity and willingness to disclose. Proceedings on Privacy Enhancing Technologies, 2, 68–94. doi:10.2478/popets-2022-0036
10. Belen-Saglam R, Nurse JRC and Hodges D (2022) An Investigation Into the Sensitivity of Personal Information and Implications for Disclosure: A UK Perspective. doi: 10.3389/fcomp.2022.908245
11. Teebken, M. & Hess, T. (2021) Privacy in a digitized workplace- Towards an understanding of employee privacy concerns (HICSS). [DOI: 10.24251/HICSS.2021.800]
12. Cella M. Sum, Caroline Shi and Sarah E. Fox. (2025). It's Always a Losing Game: How Workers Understand and Resist Surveillance Technologies on the Job, Proceedings of the ACM on Human-Computer Interaction, Volume 9, Issue 2. Article No.: CSCW004, Pages 1 – 32. https://doi.org/10.1145/3710902.
13. Voß, M., Bosak, O., Hoebertz, M., Mohsenzadeh, F., Schnebbe, M., Poeppelbuss, J., & Eisenbeiss, M. (2022). Design principles for personalized assistance systems that respect privacy. *AIS Transactions on Human-Computer Interaction, 14*(4), 461–489. https://doi.org/10.17705/1thci.00176
14. Fernandes, Teresa and Nuno Pereira (2021); Revisiting the privacy calculus: Why are consumers willing to disclose personal data online?; Telematics and Informatics, 65, 101717.
15. Meier, Y., & Krämer, N. (2024). The privacy calculus revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels. Communication Research 51(2):178-202. DOI: 10.1177/00936502221102101

16. Bhave, D. P., Teo, L. H., & Dalal, R. S. (2019). Privacy at Work: A Review and a Research Agenda for a Contested Terrain. Journal of Management, 46(1), 127-164. https://doi.org/10.1177/0149206319878254
17. Serova A.V., Shcherbakova O.V.(2022) The Employee's Right to Privacy Transformation: Digitalization Challenges. Kutafin Law Review. ;9(3):437-465. https://doi.org/10.17803/2713-0525.2022.3.21.437-465
18. Skatova A, McDonald R, Ma S, Maple C (2023) Unpacking privacy: Valuation of personal data protection. PLoS ONE 18(5): e0284581. https://doi.org/10.1371/journal.pone.0284581
19. Bruin, M., & Mersinas, K. (2024). Individual and contextual variables of cyber security behaviour: An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour. *arXiv*. https://doi.org/10.48550/arXiv.2405.16215
20. Stegman, J., Trottier, P., Hillier, C., Khan, H., & Mannan, M. (2022). "My Privacy for their Security": Employees' Privacy Perspectives and Expectations when using Enterprise Security Software. *ArXiv*, abs/2209.11878. https://doi.org/10.48550/arXiv.2209.11878.
21. Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR: Is it worth it? Perceptions of workers who have experienced its implementation. *ArXiv, abs/2405.10225*.
22. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index_IN.pdf
23. https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html
24. https://www.dsci.in/files/content/knowledge-centre/2023/Data%20Protection%20Practices%20of%20Indian%20IT-ITES%20industry_0.pdf