International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

Workplace Monitoring, Digital Tracking and Employee Privacy: A Legal Assessment

[1]Shweta Saini & [2]Dr. Shikha trivedi
[1]Ph.D. Research Scholar & [2]Assistant Professor
Department of Law
Apex University, Jaipur

Abstract
The rapid advancement of digital monitoring technologies in contemporary workplaces has created substantial legal, ethical and organizational challenges regarding employee privacy rights. This review article examines the legal landscape governing workplace monitoring across India, the European Union and the United States, analyzing statutory frameworks, regulatory enforcement and judicial precedents. The article synthesizes the Digital Personal Data Protection (DPDP) Act 2023 in India, the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, identifying common legal principles of proportionality, necessity and transparency alongside significant jurisdictional divergences. The analysis reveals that while the EU has established the most prescriptive framework with substantial enforcement mechanisms, India's DPDP Act remains nascent with significant implementation gaps and the United States presents a fragmented landscape with federal-level protection deficits. The article concludes that balanced regulatory approaches must reconcile legitimate employer interests in productivity and security with fundamental employee rights to privacy and dignity, particularly addressing emerging technologies and power imbalances inherent in employment relationships.

Keywords: employee monitoring, digital tracking, workplace surveillance, privacy rights, data protection, DPDP Act, GDPR, CCPA, employment law

INTRODUCTION

Workplace monitoring has evolved from periodic supervision into comprehensive digital surveillance systems capable of tracking employee activities with unprecedented granularity. Employers now deploy technologies monitoring email communications, internet usage, keystroke patterns, GPS location, biometric data and behavioral metrics, often with minimal transparency and limited employee oversight [1]. The proliferation of remote work accelerated by the COVID-19 pandemic has intensified monitoring adoption, with current statistics indicating that approximately 78% of organizations utilize employee monitoring software, a figure projected to reach 85-90% among large enterprises by 2025[2].

This technological capacity has substantially outpaced legal frameworks governing such practices. While employees face increasingly invasive surveillance, comprehensive legal protections remain fragmented and inadequate across most jurisdictions[3]. India, despite constitutional privacy protections recognized by the Supreme Court in 2017 and the recent

enactment of the DPDP Act 2023, lacks specific workplace monitoring standards and enforcement infrastructure[1]. The European Union, conversely, has established stringent GDPR-based protections with substantial regulatory enforcement, exemplified by the €32 million fine against Amazon France Logistique for excessive employee surveillance in January 2024[4]. The United States presents a particularly fragmented landscape where federal protections remain minimal, leaving employee privacy primarily governed by state-level legislation and litigation-driven jurisprudence[5].

This review article provides a comprehensive legal assessment of workplace monitoring across these jurisdictions, analyzing statutory frameworks, regulatory enforcement actions and emerging case law to identify common principles and critical divergences. The article demonstrates that effective workplace monitoring regulation requires balancing legitimate employer interests in productivity, security and asset protection against fundamental employee rights to privacy, dignity and autonomy. The analysis reveals that proportionality, necessity, transparency and accountability have emerged as core principles across jurisdictions, yet implementation remains inconsistent and inadequate in addressing rapid technological advancement.

Workplace Monitoring: Scope And Technologies

Workplace monitoring encompasses systematic observation and recording of employee activities, communications and productivity using digital technologies[1]. Contemporary monitoring technologies deployed across organizations include email and instant messaging surveillance, keystroke logging and screen recording, GPS location tracking, biometric identification systems, video surveillance and artificial intelligence-driven behavioral analytics that profile employee performance and predict future conduct[2]. These technologies operate on employer-provided devices and, increasingly, on personal devices through bring-your-own-device (BYOD) policies that blur boundaries between professional and personal privacy[3].

Employers justify monitoring through several business rationales: ensuring productivity optimization, protecting intellectual property and trade secrets, detecting security threats and data breaches, maintaining audit trails for regulatory compliance and identifying policy violations and misconduct[1]. However, empirical research demonstrates that comprehensive monitoring often produces counterintuitive results, with intensive surveillance correlating with reduced productivity, decreased employee morale, diminished creativity and innovation, higher turnover rates and increased stress-related health impacts[2]. The psychological effects of constant surveillance include increased anxiety, reduced autonomy perception, erosion of workplace trust and chilling effects on legitimate employee activities beyond narrow productivity metrics[1].

Beyond psychological impacts, workplace monitoring creates substantial risks for discriminatory application. Artificial intelligence-driven monitoring systems may perpetuate historical biases, producing disparate impacts on employees from protected demographic groups[3]. Comprehensive personal data collection facilities harassment, targeted discipline based on protected characteristics and other discriminatory practices. These organizational

and individual risks suggest that adequate legal protections serve not merely abstract rights principles but practical interests in employee well-being, organizational health and compliance with anti-discrimination standards[1].

Legal Framework In India

Constitutional and Statutory Foundations

India's legal approach to workplace monitoring derives from constitutional privacy protections and recently enacted statutory frameworks. The Supreme Court of India, in the landmark 2017 judgment *K.S. Puttaswamy (Deceased) through L.Rs. v. Union of India*, established privacy as a fundamental right protected under Articles 14, 19 and 21 of the Indian Constitution[1]. The Court held that privacy encompasses both personal and professional spheres, thereby extending constitutional protection to employment contexts, while recognizing that privacy rights are not absolute and may be restricted only through law satisfying tests of necessity, purpose and proportionality[1].

The Information Technology Act, 2000 (IT Act) provides the primary statutory framework addressing data processing and system security in India, though it does not explicitly address employee monitoring[1]. Relevant provisions include Section 43 establishing civil liability for unauthorized access to computer systems, Section 66 providing criminal penalties for unauthorized access and data theft and Section 72 imposing confidentiality obligations on those accessing data[1]. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) establish security obligations for entities processing sensitive personal data, requiring reasonable security practices and data protection measures[1].

The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection (DPDP) Act 2023, which became effective on August 18, 2024, represents India's first comprehensive data protection legislation with direct applicability to workplace monitoring[1]. The Act establishes fundamental principles governing personal data processing: lawfulness requiring processing to be based on lawful bases including contractual necessity, legal obligation, consent, or legitimate interest; purpose limitation restricting secondary use of data without additional legal basis; data minimization limiting collection to what is necessary for specified purposes; accuracy and quality maintenance; storage limitation requiring deletion after purposes are fulfilled; and accountability requiring documentation and risk assessments[1].

Section 7 of the DPDP Act permits processing of personal data for legitimate purposes in employment contexts without explicit consent, including fulfillment of contractual obligations, performance of legal or regulatory functions and protection of legitimate interests[1]. However, even where consent is not required, employers must comply with proportionality and necessity standards[1]. The Act grants employees specific rights including the right to access personal data collected about them, the right to correction of inaccurate information, the right to erasure where storage is no longer necessary and the right to grievance redressal through designated officers[1].

Implementation Challenges and Regulatory Gaps

Despite DPDP Act enactment, significant implementation gaps persist. The legislation provides minimal guidance regarding workplace-specific monitoring standards, proportionality thresholds, or parameters defining legitimate employer interests[1]. The Act does not establish specific standards for particular monitoring technologies or address power imbalances inherent in employment relationships where employees may lack practical ability to refuse monitoring conditions[1]. Regulatory enforcement mechanisms rely primarily on individual complaints rather than proactive regulatory oversight comparable to EU authorities[1].

The Data Protection Board of India has authority to impose substantial penalties for violations, including up to ₹250 crore for failure to implement reasonable security safeguards, ₹200 crore for non-fulfillment of obligations regarding employee data protection and ₹50 crore for failure to notify data breaches[2]. However, limited guidance exists regarding what constitutes "reasonable" measures in workplace contexts or how the Board will interpret proportionality requirements[1]. As the DPDP Act remains newly implemented, judicial interpretation addressing workplace monitoring specifically remains minimal, leaving substantial uncertainty regarding practical compliance requirements[1].

Legal Framework In The European Union

The General Data Protection Regulation

The General Data Protection Regulation (GDPR), effective May 25, 2018, represents the world's most comprehensive and prescriptive data protection legislation, establishing stringent standards for workplace monitoring[4]. The GDPR applies to employers processing employee personal data regardless of the employer's physical location, provided they offer goods or services to EU residents or monitor their behavior[4]. GDPR Article 6 establishes lawful bases for processing personal data, including consent (though disfavored in employment contexts due to power imbalances), contract, legal obligation, vital interests, public task and legitimate interests[4].

The GDPR requires employers to implement data protection by design and default, incorporating privacy-protective measures from the outset when designing monitoring systems[4]. Articles 35-36 require employers to conduct Data Protection Impact Assessments (DPIAs) when monitoring presents high risks to employee rights, documenting necessity, proportionality and safeguards. Where monitoring poses significant risks, prior consultation with supervisory authorities may be required[4]. Transparency requirements under Articles 13-14 mandate that employers provide clear information to employees regarding monitoring purposes, data categories, recipients, storage duration and employee rights[4]. The European Data Protection Board (EDPB) and national authorities have established that workplace monitoring must be proportionate, meaning the monitoring method is appropriate and necessary for stated purposes, data collection is limited to necessity, monitoring intrusiveness is balanced against identified risks and less intrusive alternatives are unavailable[4]. Covert monitoring is generally impermissible except in exceptional circumstances where criminal activity or serious misconduct is suspected[4]. Comprehensive keystroke logging and screen

recording require heightened justification due to intrusiveness and monitoring of personal communications or private devices requires explicit consent or exceptional circumstances[4].

Regulatory Enforcement and Case Law

GDPR enforcement against workplace monitoring has produced substantial precedent establishing stringent standards. The French Data Protection Authority (CNIL) imposed a €32 million fine on Amazon France Logistique in January 2024 for employee monitoring practices deemed excessive, non-transparent and violative of GDPR privacy standards[4]. The regulator found that Amazon's geolocation tracking, keystroke monitoring and performance metrics collection were disproportionate to stated security and productivity purposes, implemented without adequate transparency or employee notice and applied without sufficient safeguards[4]. This enforcement action established that even multinational corporations cannot maintain unaccountable monitoring systems without substantial regulatory consequences[4]. The H&M case exemplifies GDPR enforcement regarding inappropriate monitoring scope. Investigation revealed that H&M maintained extensive records of employee personal lives since 2014 through unlawful email monitoring, internet page tracking, phone conversation recording and video surveillance without legitimate legal basis or proper documentation[3]. These violations resulted in substantial regulatory action and public accountability, establishing precedent that comprehensive employee surveillance violates GDPR standards regardless of stated business justifications[3].

Legal Framework In The United States

Federal Protections and Limitations

The United States lacks comprehensive federal privacy legislation specifically protecting employees from workplace monitoring, resulting in a fragmented landscape where protection varies substantially by jurisdiction and employment context[5]. The Electronic Communications Privacy Act (ECPA) 1986, specifically the Wiretap Act and Stored Communications Act (SCA), provides limited protections against unauthorized interception of employee electronic communications[5]. The "business use exception" permits employers to monitor communications on employer-owned systems, but unauthorized access to communications where employees have reasonable privacy expectations remains prohibited[5]. The Computer Fraud and Abuse Act (CFAA) 1986 prohibits unauthorized access to computer systems, establishing both civil and criminal liability applicable to unauthorized employee access and data theft[5]. However, the CFAA does not restrict employer monitoring on systems employers own and control[5]. The Fourth Amendment protects against unreasonable searches by government actors but does not apply to private employers, creating a substantial protection gap in the private employment sector[5]. The Supreme Court in *United States v. Jones* (2012) established that GPS tracking constitutes a search under the Fourth Amendment, but this protection applies only to governmental surveillance, not private employer tracking[5].

California Consumer Privacy Act and State Variations

The California Consumer Privacy Act (CCPA), effective January 1, 2020, represents the first comprehensive state privacy law, with significance extending beyond California due to its

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

influence on national business practices. Importantly, the CCPA explicitly includes employees, job applicants and independent contractors within the definition of "consumers," thereby extending protections to employment contexts. The CCPA applies to for-profit employers meeting specified thresholds: annual gross revenue exceeding $25 million, buying or receiving personal information of 100,000+ consumers, or deriving 50%+ of annual revenue from selling or sharing personal information. Under CCPA, employees retain rights to know what personal information employers collect and the purposes to delete personal information subject to limited exceptions, to opt out of employers selling or sharing personal information, to correct inaccurate information and to limit use of sensitive personal information including health data, biometric data and precise location. Employers must provide privacy notices in accessible language at the time of data collection, explaining information categories, purposes and employee rights. Other states including New York, Washington and Massachusetts have enacted similar protections, creating state-level variations that complicate employer compliance for national organizations[6].

Judicial Precedent and Privacy Torts

U.S. courts have developed substantial precedent addressing workplace monitoring through various legal theories despite federal statutory gaps. The case *Pietrylo v. Hillstone Restaurant Group* (2009) involved an employer accessing an employee's personal Facebook account without authorization to investigate employee conduct. The court determined that this unauthorized access violated the Stored Communications Act, establishing that employers cannot access personal social media accounts regardless of employment-related justifications[6].

In *Arias v. Mutual of Omaha*, an employee sued for invasion of privacy and constitutional violations after discovering continuous smartphone tracking by her employer. The case attracted substantial media attention from outlets including CNN and The Guardian and was settled outside court, confirming judicial concerns about compulsory employee tracking and its relationship to unlawful termination. State privacy tort law recognizes intrusion upon seclusion as a civil wrong, requiring defendants to establish that conduct was highly offensive to reasonable persons and invaded protected privacy interests. These cases establish that despite minimal federal protections, courts recognize important employee privacy interests and are willing to impose liability for particularly invasive monitoring practices[6].

Comparative Analysis: Principles And Divergences

Common Legal Principles

Despite jurisdictional variations, fundamental legal principles regarding workplace monitoring have emerged across India, the European Union and the United States. Proportionality requires that monitoring must be proportionate to identified risks and organizational needs, with excessive monitoring impermissible regardless of stated justifications[1][4][7]. Necessity mandates that monitoring must be necessary to achieve specified, legitimate purposes, with less intrusive alternatives exhausted. Transparency requires that employees be informed before monitoring implementation about what data will be collected, why collection will occur, how data will be handled and what rights employees

retain[4][7]. Accountability requires employers to maintain documentation, conduct risk assessments and demonstrate compliance with applicable legal standards. Data security principles require that personal data collected through monitoring be protected against unauthorized access, breaches and misuse. Purpose limitation establishes that data collected for specific monitoring purposes cannot be repurposed for unrelated objectives without additional legal basis. Individual rights protection establishes that employees retain fundamental rights to access personal data collected about them, correct inaccurate information and seek deletion where storage is no longer necessary[7][8].

Jurisdictional Divergences

The three jurisdictions differ substantially in regulatory prescriptiveness. The European Union, through GDPR and EDPB guidance, establishes the most detailed standards, explicitly addressing specific technologies and requiring prior assessments before monitoring implementation, with enforcement through substantial regulatory fines and mandatory compliance measures[4]. The United States presents a moderate but fragmented approach where federal law provides minimal protection, creating variation across state jurisdictions, with development occurring primarily through litigation rather than proactive regulatory standard-setting[7]. India presents the least prescriptive framework, with DPDP Act establishing general principles but providing minimal guidance specific to workplace monitoring and significant interpretive development remaining necessary as regulatory infrastructure continues developing[1]. Regarding employee consent, the EU explicitly recognizes that employment power imbalances undermine consent validity, discouraging reliance on consent as the sole lawful basis[4]. The United States generally permits consent-based monitoring, though some jurisdictions recognize limitations where consent is procured through coercion[5,7]. India's DPDP Act permits processing for legitimate employment purposes without explicit consent but does not specifically address consent validity under employment power imbalances[8]. For monitoring of personal communications, the EU establishes strict limitations requiring heightened justifications, with monitoring of personal email or communications generally impermissible except under exceptional circumstances. The United States permits monitoring on employer-provided systems under business use exceptions, though courts recognize privacy interests where employees have reasonable expectations of privacy[5]. India permits internet activity monitoring under Section 69A of the IT Act, though courts may apply constitutional privacy protections to limit monitoring of clearly personal communications[9].

Psychological And Organizational Impacts

Beyond legal analysis, empirical research documents substantial impacts of workplace monitoring on employee psychology and organizational outcomes. Comprehensive monitoring correlates with increased stress and anxiety, reduced autonomy perception, diminished morale and job satisfaction, reduced willingness to engage in legitimate collaborative and developmental activities and erosion of trust between employers and employees]. These psychological effects translate into organizational consequences including decreased overall productivity (contrary to employer assumptions), reduced creativity and

innovation necessary for competitive advantage, higher employee turnover increasing recruitment and training costs and decreased organizational commitment and engagement with organizational goals[1][10].

The mechanisms of productivity paradox operate through employees focusing on appearing productive according narrow surveillance metrics rather than engaging in substantive work that benefits organizations long-term[1]. Surveillance environments inhibit creative thinking, experimentation and innovation necessary for organizational competitiveness. Employees under intensive monitoring demonstrate higher rates of anxiety disorders, depression and burnout in longitudinal studies[2]. These empirical findings suggest that employee protection through adequate legal frameworks serves not merely abstract rights principles but practical interests in organizational health, employee well-being and competitive effectiveness[10].

Workplace monitoring systems incorporating artificial intelligence present specific discrimination risks, with algorithmic systems potentially perpetuating historical biases and producing disparate impacts on employees from protected demographic groups[3]. Comprehensive personal data collection can facilitate workplace harassment, targeted discipline based on protected characteristics and other discriminatory practices[3]. These risks suggest that data protection frameworks must specifically address algorithmic monitoring and discrimination prevention[10].

Regulatory Gaps And Implementation Challenges

India-Specific Gaps

Despite DPDP Act enactment, significant regulatory gaps persist in India. The legislation does not establish workplace-specific monitoring standards, proportionality thresholds, or parameters defining legitimate employer interests in particular monitoring contexts. Implementation guidance from the Department for Promotion of Industry and Internal Trade (DPIIT) remains limited, leaving employers and employees uncertain about compliance requirements. The regulatory framework does not adequately address power imbalances inherent in employment relationships where employees may face practical inability to refuse monitoring conditions tied to employment continuation.

Limited guidance addresses emerging monitoring technologies including artificial intelligence-driven behavior prediction systems, biometric monitoring and wearable tracking devices. The DPDP Act relies primarily on individual complaints for enforcement rather than proactive regulatory investigation comparable to EU authorities, limiting practical deterrence for non-compliant employers. As the Act remains newly implemented with limited case law, substantial uncertainty persists regarding how courts and regulators will interpret proportionality and necessity requirements in specific workplace contexts[10].

United States Fragmentation

The U.S. regulatory landscape presents significant fragmentation challenges. Wide variations across states in privacy protections create compliance burdens for national employers and unpredictability regarding applicable standards[5]. Federal statutory gaps leave significant protection gaps particularly in states without comprehensive privacy legislation, with only California, New York, Washington and Massachusetts providing substantial employee

protections. Privacy protections emerge through costly litigation rather than proactive regulatory standard-setting, creating incentives for employers to test legal boundaries and defer compliance until litigation forces change. Rapid technological development outpaces legal framework development, with monitoring technologies advancing faster than statutory and judicial responses, creating persistent protection gaps for emerging surveillance methods. This fragmentation suggests that federal legislative action establishing baseline employee protections would benefit both employers seeking clarity and employees seeking consistent protections[6].

EU Enforcement Variation

Despite GDPR's prescriptive framework, challenges persist. While GDPR established uniform standards, enforcement varies across member states based on resource allocation and regulatory priorities, with some authorities more active than others in investigating and sanctioning monitoring violations. Emerging monitoring technologies including artificial intelligence, biometric systems and predictive analytics present novel challenges that existing frameworks address inadequately. Cross-border employee data transfers create complexity regarding applicable jurisdictions and standards for multinational organizations. GDPR compliance requirements create substantial costs for employers, particularly smaller organizations, potentially disadvantaging small business sectors relative to large corporations with dedicated compliance infrastructure[3][4].

Recommendations For Balanced Regulation

Effective workplace monitoring regulation must balance legitimate employer interests in productivity, security and asset protection against fundamental employee rights to privacy, dignity and autonomy. For India, regulatory authorities should develop detailed workplace-specific guidance establishing proportionality standards and monitoring thresholds, create robust Data Protection Board enforcement mechanisms with proactive investigation authority, address employment power imbalances through legal presumptions that certain monitoring practices violate employee rights absent exceptional justification, develop technology-specific standards for emerging monitoring systems and establish employee consent protections recognizing that employment dependence undermines consent voluntariness[9].

The United States should enact comprehensive federal baseline privacy legislation establishing minimum employee protections applicable nationwide while permitting states to impose stricter standards, develop sector-specific standards for sensitive employment contexts including healthcare and legal services, establish technology-specific requirements for emerging monitoring systems, create administrative enforcement mechanisms beyond litigation and mandate clear, accessible employee notices regarding monitoring practices and rights[10].

Across jurisdictions, harmonization efforts should establish principles-based standards establishing core principles of proportionality, necessity, transparency and accountability while permitting jurisdictional implementation flexibility, develop mutual recognition frameworks permitting multinational employers to comply through unified, highest-standard approaches, establish shared best practices forums for regulatory experience-sharing, develop

international standards addressing monitoring of emerging technologies before national framework fragmentation intensifies further and establish international consensus on minimum employee rights reflecting fundamental human rights principles[4][5][10].

Conclusion

Workplace monitoring has become widespread due to technological advances and organizational demands for efficiency, yet legal regulation remains uneven and underdeveloped across jurisdictions. While India, the European Union and the United States share common principles such as proportionality, transparency and accountability, they differ significantly in regulatory depth and enforcement. The European Union provides the strongest employee protections through the GDPR, the United States relies largely on fragmented state laws and litigation and India's DPDP Act establishes only a foundational framework requiring further development. Evidence shows that excessive monitoring can undermine employee trust, autonomy, well-being and innovation, highlighting the practical importance of robust legal safeguards. Addressing these challenges requires comprehensive, balanced regulation that protects employee dignity and rights while accommodating legitimate employer interests, with proactive legal development needed to keep pace with advancing monitoring technologies.

References

[1] Gupta, N., & George, A. (2025). Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. In *Data Governance and the Digital Economy in Asia* (pp. 34-53). Routledge.

[2] MeraMonitor. (2025, July 24). Employee Monitoring Laws in India 2025. Available at : https://meramonitor.com/employee-monitoring-laws-in-india/

[3] Zunic Law. (2020, October 7). H&M GDPR Breach: Employee Monitoring Case Study. Available at: https://zuniclaw.com/en/hm-gdpr-breach/

[4] Arthur Cox. (2025, February 2). Employee Monitoring at Work: Regulatory Enforcement Actions Against Excessive Employee Monitoring practices continue. Available at: https://www.arthurcox.com/knowledge/employee-monitoring-at-work-regulatory-enforcement-actions-against-excessive-employee-monitoring-practices-continue/

[5] Flowace AI. (2025, September 22). Employee Monitoring Laws: Legal Guide 2026. Available at: https://flowace.ai/blog/employee-monitoring-laws/

[6] Berkeley Labor Center. (2023, December 6). Overview of New Rights for Workers Under the California Consumer Privacy Act. Available at: https://laborcenter.berkeley.edu/overview-of-new-rights-for-workers-under-the-california-consumer-privacy-act/

[7] Kumari, S. (2025, December 4). Digital Privacy Rights in the Workplace: Balancing Employee Protection with Employer Surveillance Needs. Available at: https://recordoflaw.in/digital-privacy-rights-in-the-workplace-balancing-employee-protection-with-employer-surveillance-needs/

[8] Privacy Pillar. (2024, August 13). Employee Privacy Rights and Workplace Monitoring. Available at: https://privacypillar.com/employee-privacy-rights-and-workplace-monitoring/

[9] Apploye. (2025, October 17). Employee Monitoring Statistics: Shocking Trends in 2025. Available at: https://apploye.com/blog/employee-monitoring-statistics/

[10] Gallagher, E. (2023, October 19). Key Employer Obligations Under India's New Data Protection Legislation. Available at: https://knowledge.dlapiper.com/dlapiperknowledge/globalemploymentlatestdevelopments/india-key-employer-obligations-under-indias-new-data-protection-regime