Newsletter

11th Edition | January 2026 | Salot and Shah Associates

SALOT & SHAH ASSOCIATES

Address: 503, 5th Floor, Phoenix Towers, Opp New Girish Cold Drinks, Vijay X Roads, to, Commerce Six Road, Navrangpura, Ahmedabad, Gujarat - 380009.

91 - 93286 69090

info@salotandshah.com

www.salotandshah.com

Welcome to the 11th edition of the Salot and Shah Associates Newsletter. We are pleased to continue our effort of keeping our clients, associates, and readers informed about important legal developments, emerging trends, and practical insights from across the legal landscape.

In this edition, we bring you concise updates, expert perspectives, and thoughtful commentary on matters that impact businesses and individuals alike. Our aim is to simplify complex legal issues, highlight regulatory changes, and share knowledge that supports informed decision-making in an ever-evolving legal and commercial environment.

As always, this newsletter reflects our commitment to clarity, relevance, and professional excellence. We thank you for your continued trust and engagement, and we look forward to sharing valuable insights with you in this edition.

OVERVIEW

Rethinking Employee Monitoring Through Indian Labour Jurispruedence in the Era of the new Labour Codes

- Surveillance or a Safegaurd ?

Navigating the New Normal: AI Governance & Legal Liability in Business

- A global outlook upon the AI Compliance and Redressal

2025: When Law and Policy Redefined India's Digital Economy

- A overview of the overall legal impacts in digital economy of India in 2025

RETHINKING EMPLOYEE MONITORING THROUGH INDIAN LABOUR JURISPRUDENCE IN THE ERA OF THE NEW LABOUR CODES: SURVEILLANCE OR SAFEGUARD ?

INTRODUCTION

The modern workplace has undergone major changes during this time. The proliferation of remote work, hybrid employment structures, and digital collaboration across the globe upon such collaborative platforms has altered how labor work is performed, supervised, and assessed. Additionally the physical proximity after once the foundation of management oversight, has been superseded by algorithmic supervision and digital monitoring. Employee monitoring the systematic observations, recordings, and analysis of employee behavior characteristics during working hours has developed as a strong managerial tool in today's changing and challenging business ecology. New advancements in labor legislation bring about a new changing form of workplace supervision.

Employers consider such surveillance as necessary to ensure productivity, data security, and regulatory compliance, but the practice presents serious legal and constitutional challenges. In India, these challenges are issues which are heightened under the constitutional right to privacy, which was recognized as a basic right in Justice K.S. Puttaswamy v. Union of India (2017), as well as the expanding framework of labour legislation under the four new Labour Codes. The essential question, therefore, is not whether employee monitoring is permissible, but to what extent it can be lawfully exercised without jeopardizing workers' dignity, autonomy, and privacy.

This article will critically evaluate the employee monitoring mechanism in light of Indian labour law jurisprudence as in accordance with the constitutional principles, and in alignment with the newly established Labour Codes, with the goal of striking a balance between managerial authority and employee rights.

UNDERSTANDING EMPLOYEE MONITORING IN CONTEMPORARY EMPLOYMENT

Employee monitoring refers to a variety of tactics used by businesses to supervise employee conduct. These include time-tracking software, keyboard logging, email scanning, video

surveillance, biometric attendance systems, and productivity analytics.

In remote and hybrid contexts, monitoring frequently extends into digital domains that intersect with an employee's personal domain, putting a very fine line of distinction between professional supervision and personal life.

Traditionally, today the management supervision has been permitted under Indian labour law as part of the employer-employee relationship. However, this oversight authority has never been absolute. The judicial decisions consistently recognize that discipline must adhere to the principles of fairness, rationality, and withhold the principles of natural justice. The arrival of invasive technology requires a re-evaluation of these limits.

THE OBJECTIVES INCLUDE PRODUCTIVITY, SECURITY & ACCOUNTABILITY.

From the employer's perspective, employee monitoring is driven by three principal objectives.

1. **Enhancing Productivity**

In a remote-first setting, employers frequently use digital monitoring technologies to replace physical supervision.

Time-tracking software, login duration analysis, digital attendance maintenance and job production measures are utilized to keep employees interested during the workday. Employers believe that such monitoring maintains organizational efficiency and avoids the abuse of paid time. Indian courts have always recognized reasonable monitoring as a lawful managerial responsibility. However, extensive or constant monitoring might cross the line into arbitrariness, especially if it ignores the nature of the activity or sets unreasonable performance goals.

2. **Protection of Sensitive Information**

Increased digitization increases the risk of data breaches, intellectual property theft, and cyber espionage. Employers, particularly in the financial, healthcare, and technology industries, use monitoring systems to identify unauthorized access, data leaks, and policy breaches. Contract law and industrial jurisprudence both accept the employer's obligation to preserve sensitive information. However, this obligation must be implemented in a balanced manner, ensuring that monitoring methods are targeted rather than indiscriminately obtrusive.

3. **Ensuring Accountability and Legal Compliance**

Certain sectors have rigorous regulatory systems that need internal monitoring and audit trails. In such instances, employee surveillance is not optional, but rather part of the statutory compliance requirements. Nonetheless, even compliance-driven monitoring must follow constitutional safeguards and labor law

The Puttaswamy judgment revolutionized Indian labor relations by elevating privacy to a fundamental right under Article 21, subjecting employer surveillance to a rigorous three-pronged test of legality, legitimate aim, and proportionality to ensure that monitoring remains minimally intrusive and constitutionally valid.

Employee Monitoring Under the New Labor Codes

The implementation of the four Labour Codes includes namely, the Code on Wages, 2019, the Industrial Relations Code, 2020, the Occupational Safety, Health, and Working Conditions Code, 2020, and the Code on Social Security, 2020, indicates a trend toward labor law consolidation and modernization. While these Codes specifically limit employee monitoring, their rules have substantial immediate consequences.

Industrial Relations Code, 2020 : The code strengthens the obligation for standing orders for businesses that exceed the prescribed threshold. Standing orders control job circumstances such as disciplinary action and misbehavior. Any method of employee monitoring that might result in disciplinary action must be explicitly stated in verified standing orders. Failure to reveal monitoring techniques may make disciplinary hearings open to dispute on procedural unfairness and violations of natural justice.

Occupational Safety, Health, and Working Conditions Code, 2020: This Code highlights the employer's responsibility to provide a safe and compassionate workplace. Psychological well-being, while not expressly defined, is increasingly recognized as a component of occupational health. Excessive monitoring that causes stress, worry, or a hostile work environment may be in conflict with the spirit of this Code.

Code on Wages, 2019: This code helps in monitoring systems for assessing attendance, working hours, and productivity have a direct impact on salary setting. Any technology system that erroneously tracks labor hours or unfairly penalizes employees can lead to pay disputes and statutory violations.

Judicial Trends in Indian Labour Law: The shift in Indian labor law reflects a broader constitutional move toward protecting individual agency within the workplace. Modern labor tribunals and High Courts increasingly treat the employee not

merely as a tool of production, but as a citizen entitled to a "reasonable expectation of privacy."

This means that while an employer's right to protect property is valid, it does not grant them absolute dominion over an employee's digital or physical movements. By insisting that surveillance be transparent and limited to "public" work spheres, the judiciary ensures that the power dynamic between capital and labor remains balanced, preventing workplace monitoring from devolving into psychological coercion or a violation of human dignity.

In Indian labor jurisprudence, the Principle of Informed Consent and Transparency serves as a vital safeguard against the overreach of managerial prerogative. While the traditional power dynamic in an employment contract is inherently skewed—often making "consent" more of a formal requirement than a truly voluntary choice—courts have pivoted toward transparency as the primary equalizer. Under the evolving framework of the Digital Personal Data Protection Act (DPDP) 2023 and the foundational "Right to Privacy" established in K.S. Puttaswamy, employers are increasingly held to a standard of "Notice-and-Purpose." This means monitoring is only legally sustainable when it is conducted for a specific, lawful purpose, is strictly time-bound in its data retention, and is clearly communicated to the workforce to prevent the arbitrary exercise of disciplinary power.

Balancing Managerial Authority and Employee Dignity: Employee monitoring, when used responsibly, can serve as a safeguard rather than a surveillance tool. The distinction rests in intention, design, and implementation. Monitoring that targets particular dangers, is restricted in scope, and respects privacy is more likely to withstand legal scrutiny.

Employers must understand that their employees are more than just productivity units; they are persons with rights and dignity. Indian labour law, bolstered by constitutional values and the new Labour Codes, requires a balanced approach that considers both economic efficiency and human rights.

CONCLUSION

As Indian workplaces evolve, the law must change to govern new types of digital surveillance. While the new Labour Codes provide a contemporary structural framework, the lack of specific legislation on employee monitoring increases employers' obligation to self-regulate in conformity with constitutional norms. As the government implements new labor laws, the legislative intent shifts toward a rights-respecting monitoring structure.

Employee surveillance cannot be considered an unfettered management privilege. It must function within a framework of legality, proportionality, and justice, guided by the right to privacy and worker welfare goals. Finally, the validity of workplace surveillance rests on legal constraint and ethical responsibility, rather than technological capabilities. In rethinking employee monitoring, Indian labour law sends a clear message: efficiency must coexist with dignity, and surveillance must never trump fundamental right.

NAVIGATING THE NEW NORMAL : AI GOVERNANCE & LEGAL LIABILITY IN BUSINESS

INTRODUCTION

Artificial Intelligence (AI) has quickly evolved from a sci-fi idea to a vital part of contemporary corporate operations. Businesses in almost every industry are utilizing AI to increase productivity and obtain a competitive edge, whether it be through automated decision-making systems, predictive analytics, or chatbots for customer support. Regulators have taken note of this increase in AI adoption, though. Businesses are now subject to more scrutiny and legal exposure as AI plays a bigger role in decision-making. As legal frameworks that seek to regulate AI development, implementation, and accountability begin to take shape in 2025, legal and compliance teams must pay close attention to AI governance.

GLOBAL ADOPTION OF AI

The EU's Artificial Intelligence Act, which is scheduled to go into effect by the end of this year, is among the most important developments. The law establishes a risk-based categorization of AI systems and imposes strict compliance requirements on "high-risk" applications like credit scoring systems, automated hiring tools, and biometric surveillance. Although federal AI regulation in the US is moving more slowly, several states, including California and New York, have introduced laws aimed at addressing algorithmic bias, consumer rights, and AI transparency. Asia's more innovative regulatory models, which combine targeted oversight with voluntary codes, are being adopted by nations like Singapore and Japan. These diverse strategies are united by an increasing focus on accountability, transparency, and the moral application of data in AI systems.

In the Indian context, regulators have also begun to articulate expectations for responsible AI deployment, particularly within the financial sector. The Reserve Bank of India has emphasized the importance of ethical and accountable use of artificial intelligence through its FREE-AI (Framework for Responsible and Ethical Enablement of Artificial Intelligence) initiative. The framework highlights foundational principles such as trust, fairness, accountability, explainability, and system resilience, underscoring that AI-driven decisions must remain subject to meaningful human oversight.

The RBI's approach further stresses that responsibility for AI outcomes lies with the regulated entity deploying the system, rather than with the technology itself. Organizations are expected to adopt strong governance structures, ensure transparency in AI-assisted decision-making, maintain robust data management practices, and implement mechanisms for monitoring, auditing, and addressing risks throughout the AI lifecycle. This regulatory perspective reinforces the broader global trend toward placing legal and ethical accountability at the center of AI adoption, particularly in high-impact sectors such as banking, lending, and financial services.

This regulatory emphasis aligns with guidance emerging in India, where the Reserve Bank of India has underscored ethical AI use, institutional accountability, and human oversight as core expectations for AI deployment in the financial sector.

From the standpoint of legal liability, companies are increasingly exposed to risks in three main areas. First, prejudice and discrimination are serious issues, especially when AI systems are applied to healthcare, lending, or employment decisions. Even if a biased algorithm was accidentally used, a

company could still be held accountable for discriminatory results. Second, one of the biggest exposure points is still data privacy. Massive datasets are frequently used by AI systems, and any improper use or handling of personal data may result in legal repercussions under regulations such as the California Civil Code or the GDPR in Europe. Third, businesses need to think about product liability and negligence. Courts may hold companies liable for inadequate testing or oversight if an AI tool produces harmful results, whether through incorrect recommendations, safety lapses, or erroneous outputs.

To stay ahead of the curve in light of these developments, compliance officers and in-house legal teams need to take immediate action. Mapping the organization's AI usage and its locations is the first step. After that, a comprehensive risk assessment ought to be carried out in order to pinpoint operational, ethical, and legal weaknesses. Establishing robust governance policies is also essential; this entails creating internal review committees, moral AI standards, and continuous monitoring procedures. Last but not least, maintaining compliance and risk mitigation requires keeping up with changing laws and court decisions.

CONCLUSION

In conclusion, AI creates complicated legal issues in addition to offering countless chances for innovation and development. As regulatory frameworks continue to evolve, proactive governance and legal preparedness will be key to safely navigating the AI-powered future of business.

2025: WHEN LAW AND POLICY REDEFINED INDIA'S DIGITAL ECONOMY

INTRODUCTION

For many years, India's digital economy grew much faster than the laws meant to regulate it. Mobile applications reached millions of users within months, while legal frameworks took years to develop. Technology companies experimented freely with business models, data collection, and online services, often without clear regulatory boundaries. Innovation led the way, and law followed at a distance, trying to respond after problems had already surfaced. This gap created both opportunity and uncertainty of opportunity for rapid growth, and uncertainty for users, businesses, and regulators alike. In 2025, this long-standing pattern began to change. The shift did not come through sudden or extreme measures, but through careful and steady reform. Law and policy started to reflect the real scale of India's digital life. Regulators moved beyond reacting to disputes and crises and began shaping how digital markets should function. The emphasis shifted from permitting unrestricted expansion to creating a balanced system where growth could continue within defined legal limits. The idea was no longer to control technology, but to ensure that its development remained responsible and accountable.

What emerged from this approach was not a hostile environment for innovation, but a guiding framework for it. Legal oversight became clearer and more organized across multiple sectors. Personal data was treated as a protected legal interest rather than a mere commercial resource. Online trade began to be viewed through the lens of consumer protection. Digital finance was brought closer to formal financial regulation. Even emerging technologies such as artificial intelligence entered legal discussion, with attention given to fairness and accountability. Regulation became more visible and more consistent, sending a signal that digital activity was now firmly within the scope of public law. By the end of 2025, India's digital economy no longer appeared as an unregulated space driven only by speed and scale. It began to resemble a structured marketplace governed by rules and responsibilities. Platforms were no longer just technical intermediaries, and users were no longer passive participants.

Rights, duties, and standards started defining digital relationships. The year marked a transition from experimentation to establishment, where innovation continued, but within a system shaped by legal order rather than operating outside it.

1. Personal Data Became a Matter of Legal Duty

Data has always been at the centre of the digital economy. Every click, search, payment, and preference creates information that businesses rely on to design products, target customers, and assess risk. Advertising depends on user behaviour, financial services depend on transaction records, and platforms depend on personal profiles to function efficiently. For a long time, this information was viewed mainly as a business resource that is something to be collected, analysed, and used with very few formal limits. The legal value of personal data was secondary to its commercial value. By 2025, this understanding began to change in a meaningful way. With data protection rules becoming operational, organizations were required to treat personal information as something held in trust, not merely owned. Consent could no longer be assumed through silence or technical formality. It had to be clearly obtained and capable of being withdrawn.

Companies were expected to collect only what was necessary, use it only for stated purposes, and store it only for as long as required. Practices that were once routine, such as unlimited retention or vague privacy policies, came under closer legal examination.

This legal shift also altered how digital businesses were organised internally. Technology teams had to design systems that allowed users to actively agree to data use instead of being automatically included. Human resource departments had to reassess how employee records, identity documents, and performance data were stored and shared. Customer support units were no longer only service providers; they became part of the compliance structure by handling requests for access, correction, and deletion of personal information. Data protection was no longer confined to legal departments as it spread across the entire organization. Most importantly, individuals gained formal recognition within the digital system. Their data was no longer an invisible by-product of online activity. It became something tied to legal rights as in the right to know how information is used, the right to refuse certain uses, and the right to demand correction where records are wrong. This altered the balance between platforms and users, placing personal information within the sphere of legal protection rather than pure commercial exploitation.

This development provided the foundation for many of the regulatory changes that followed in 2025. Once personal data acquired legal status, other areas of the digital economy could no longer operate without accountability. Online trade, financial technology, and automated decision-making all depended on data, and therefore all became subject to legal discipline. In this way, the protection of personal information became the starting point for bringing the wider digital economy into a regulated and structured environment.

2. Platform Power Was Treated as Market Influence:

Over time, major digital platforms turned into central access points for buying, selling, communication, and information sharing. Businesses depended on them to reach customers, and users relied on them for everyday services. Because of their enormous reach, these platforms gradually began influencing how markets operated, often without openly presenting themselves as decision-makers. Their technical systems, especially search functions and recommendation tools, quietly shaped which products, services, and voices received attention. In 2025, this situation began to attract serious legal and policy scrutiny. Regulators started looking beyond the sheer size of digital companies and focused instead on the power they exercised through control over digital access. Features such as search results, app store approvals, and algorithm-based rankings were no longer treated as neutral technical arrangements. They came to be understood as business mechanisms that could affect competition by favouring some participants over others.

This led to an important change in how digital enterprises were viewed under the law. They were no longer seen merely as technology providers offering services to users. Instead, they were increasingly regarded as organizers of digital markets, with the ability to influence economic outcomes through their internal rules and systems. For small and emerging businesses, this shift created room for legal protection against unfair or exclusionary practices. It acknowledged that competition in digital markets can be affected not only by pricing, but also by visibility and access. For large platforms, it introduced a responsibility to explain and justify decisions that shaped market participation, particularly where those decisions could restrict or disadvantage competitors.

The objective of regulation was not to break apart digital

platforms or to halt their growth. Rather, it was to prevent hidden control from deciding who succeeds and who fails in the digital marketplace. Law sought to ensure that technological systems did not become silent gatekeepers of competition, but operated within principles of fairness and accountability.

3. Digital Finance Entered a Regulated Phase of Growth:

Digital financial services had already become part of daily life in India through instant transfers, mobile payment platforms, and app-based lending. What once felt experimental had, by 2025, become routine. People used digital tools for shopping, savings, and borrowing without thinking twice. With this widespread use came a growing need for order and consistency in how such services were governed. As the sector matured, regulators moved to strengthen oversight. Financial authorities emphasized that digital payment and lending platforms must operate by the same standards of openness and responsibility that apply to conventional banks and financial institutions. Requirements relating to how customers are informed, how financial data is stored, and who bears responsibility for transactions were made more stringent and precise.

These changes led to noticeable adjustments within the industry. Lending platforms were required to present interest rates and repayment terms in a clearer and more understandable manner. Payment service providers had to improve their operational safeguards and meet higher compliance benchmarks. Access by third parties to sensitive financial information was restricted to prevent misuse and unauthorized sharing. The intention behind these measures was not to slow down innovation in digital finance, but to place it firmly within the established financial regulatory structure. Digital services could no longer operate in isolation from the rules that govern money and credit. As a result, users benefited from stronger protections, companies gained clearer legal limits, and the financial system as a whole became more secure and dependable.

4. Online Commerce Became a Consumer Law Subject:

Online marketplaces had significantly changed how people shopped. Everyday items such as food supplies, clothing, and electronic goods were increasingly purchased through digital platforms rather than from physical stores. For many consumers, these platforms became the primary point of contact for buying and selling. What began as a convenience gradually became the normal way of doing business. By 2025, this change in consumer behavior started receiving proper legal recognition. Online trade was no longer treated merely as a technological service supported by software and logistics. It was recognized as a form of consumer commerce carried out through digital channels. This shift brought with it new legal expectations relating to openness and responsibility. Platforms were required to clearly identify sellers, disclose key transaction details, and provide effective systems for addressing customer complaints.

These legal expectations produced noticeable changes in how platforms operated. Sales strategies were examined more carefully to ensure they did not mislead buyers. Practices that favored certain sellers or products drew regulatory attention. User agreements and purchase conditions had to be written in simpler and fairer terms so that customers could understand their rights and obligations. As a result, the legal relationship between platforms, merchants, and consumers became more clearly defined. The rules governing online trade were no longer set only by private platform policies. They were shaped by public law standards. This helped build confidence in digital marketplaces and confirmed that online purchases create binding legal commitments in the same way as transactions made in physical shops.

5. Telecom and Connectivity Laws Were Aligned with Digital Use:

All digital services ultimately rely on physical communication networks to function. Data travels through cables, towers, and servers before it reaches users. For a long time, however, telecom laws were designed mainly for traditional voice communication and did not fully reflect how people now communicate through internet-based services. As 2025 passed by, this gap between technology and regulation began to close. Legal and policy frameworks started recognizing that the primary role of telecom infrastructure was no longer to carry phone calls, but to support data-driven communication. Rules and guidelines were adjusted to match the reality that messaging apps, video calls, and online platforms had become the main channels of interaction.

This shift created greater coherence between infrastructure policy and digital services. Service providers received clearer guidance on their obligations, and long-term planning for networks became more closely linked with the needs of the digital economy. Regulation no longer trailed behind innovation but moved alongside it. As a result, connectivity came to be viewed as more than a basic utility. It was acknowledged as an essential and regulated foundation of the digital economy, supporting everything from online commerce to digital governance and public services.

CONCLUSION

The year 2025 is likely to be remembered as the moment when India's digital economy moved into a new stage of maturity. It was no longer defined only by how fast companies could grow or how widely technology could spread. Instead, it began to take shape within a framework of responsibility and legal order. Personal data came to be treated as something protected by law. Digital platforms were expected to follow fair market practices. Online financial services were placed within clear regulatory boundaries. Consumers, in turn, gained rights that could be enforced rather than merely promised.

This change did not happen through sudden or extreme measures. It unfolded gradually and with purpose. The digital economy did not lose its energy or ambition, but it gained structure.

Innovation continued, but it was no longer floating without limits. It began operating on a foundation of defined rules and recognized duties.

As India's digital future continues to develop, new technologies and business models will now grow within this legal framework rather than beyond it. Expansion will not come at the cost of accountability. Progress will move alongside regulation instead of outrunning it. In this sense, 2025 did not bring India's digital economy to a halt. It gave it shape, stability, and legal form.

*****