

---

# SURVEILLANCE, DATA PRIVACY AND THE WORKPLACE: HUMAN RIGHTS GAPS IN THE NEW LABOUR FRAMEWORK

---

Nikhil Kumar Jha, National Law Institute University, Bhopal

Aditya Mishra, National Law Institute University, Bhopal

## ABSTRACT

India's four Labour Codes of 2020 consolidate twenty-nine central statutes into a rationalised legislative framework but contain no express provision regulating employer surveillance, employee monitoring, or worker data rights. This paper argues that this omission, compounded by the structural limitations of the Digital Personal Data Protection Act, 2023, produces a human rights deficit that is constitutionally untenable under the proportionality standard established in *K.S. Puttaswamy v. Union of India*. Digital monitoring technologies, including biometric attendance systems, GPS tracking, productivity-scoring applications, and algorithmic management platforms, have proliferated across the Indian workplace, yet the legal architecture governing their deployment remains fragmented, consent-dependent, and practically unenforceable. The deficit falls disproportionately on gig, platform, and fixed-term contract workers, who are simultaneously the most intensively surveilled and the least protected category under both the Labour Codes and the DPDP Act. Drawing on the ILO Code of Practice on Workers' Personal Data (1997), the EU General Data Protection Regulation, and the EU Platform Work Directive (2024), this paper identifies three axes of necessary reform: worker-specific rules under the DPDP Act, a statutory right against solely automated employment decisions, and an employment-necessity standard for data collection. A draft model clause operationalising these reforms is proposed for incorporation into standing orders, platform aggregator contracts, and DPDP rules.

**Keywords:** Workplace Surveillance, Worker Data Rights, Digital Personal Data Protection Act 2023, Algorithmic Management, Labour Codes 2020, Platform Work, Gig Economy, Informational Privacy

## I. Introduction

Consider a delivery worker in Bengaluru who begins his shift by logging into a platform application that simultaneously records his GPS coordinates, tracks his delivery speed, and scores his performance in real time. His earnings, task allocation, and continued engagement on the platform are governed entirely by an algorithm he cannot see, question, or appeal. He generates vast volumes of personal data every working hour, yet no statute prescribes how that data may be collected, retained, shared, or deployed against him. This is not an isolated anomaly; it is the constitutive condition of platform labour in contemporary India.

India's four Labour Codes of 2020, namely the Code on Wages, the Industrial Relations Code, the Code on Social Security, and the Occupational Safety, Health and Working Conditions Code, represent the most significant consolidation of Indian labour law in a generation, merging twenty-nine central statutes into a rationalised framework.<sup>1</sup> Yet this sweeping reform carries a conspicuous omission: none of the four Codes contains any express provision regulating employer surveillance, employee monitoring, or worker data rights.<sup>2</sup> This lacuna carries constitutional weight. In *K.S. Puttaswamy v. Union of India*, a nine-judge bench of the Supreme Court held privacy to be a fundamental right under Article 21, encompassing informational self-determination and requiring any encroachment to satisfy a strict proportionality standard.<sup>3</sup> The pervasive digital surveillance of workers has never been tested against this constitutional threshold.

The Digital Personal Data Protection Act, 2023 ("DPDP Act") offers a partial legislative response, recognising employers as Data Fiduciaries and workers as Data Principals with rights of access, correction, and erasure.<sup>4</sup> However, the broad "legitimate use" exception under Section 7 permits processing without explicit consent in employment contexts, structurally negating meaningful consent in an inherently asymmetric power relationship.<sup>5</sup> The Act further

---

<sup>1</sup> Code on Wages, No. 29 of 2019 (India); Industrial Relations Code, No. 35 of 2020 (India); Code on Social Security, No. 36 of 2020 (India); Occupational Safety, Health and Working Conditions Code, No. 37 of 2020 (India).

<sup>2</sup> See generally India's New Labour Codes: A Critical Appraisal, Sabrang India (Dec. 18, 2025), <https://sabrangindia.in/indias-new-labour-codes-a-critical-appraisal/>; India's New Labour Codes: Assault on Workers' Rights, Janata Weekly (Nov. 29, 2025), <https://janataweekly.org/indias-new-labour-codes-assault-on-workers-rights-5-articles/>.

<sup>3</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, para. 180 (India).

<sup>4</sup> Digital Personal Data Protection Act, No. 22 of 2023, §§ 8, 11-12 (India) [hereinafter DPDP Act].

<sup>5</sup> Id. § 7; see also Vidhi Centre for Legal Policy, India's Data Privacy Law Loopholes: Are YOUR Workplace Rights Protected?, Whalesbook (Dec. 11, 2025), <https://www.whalesbook.com> (noting that the Section 7 carve-out effectively immunises employers from the consent framework in routine data-processing operations).

provides no right against solely automated decision-making, leaving workers vulnerable to algorithmic deactivation and wage deductions with no statutory avenue for human review or redressal.

This paper argues that the Labour Codes' silence, compounded by the DPDP Act's structural limitations, produces a human rights deficit that falls hardest on gig, platform, and precarious workers. By engaging constitutional doctrine, statutory critique, and comparative frameworks drawn from ILO standards and the EU General Data Protection Regulation, this paper contends that targeted legislative intervention is indispensable to protect worker autonomy and dignity in the digitised workplace. The paper proceeds in seven substantive parts, culminating in a draft model clause for worker data protection.

## **II. The New Labour Framework: Consolidation Without Rights-Protection**

The four Labour Codes of 2020, notified into force on November 21, 2025, represent India's most sweeping restructuring of labour jurisprudence since Independence, collapsing twenty-nine central statutes into a rationalised legislative architecture.<sup>6</sup> Yet the consolidation is not neutral: critics across the ideological spectrum have characterised it as a structural reorientation of the state's role from worker protection to employer facilitation, effected through a series of threshold expansions, enforcement dilutions, and definitional silences that individually appear technical but cumulatively dismantle a century of adjudicated rights.<sup>7</sup>

### **Retrenchment Thresholds and Standing Orders**

The Industrial Relations Code, 2020, raises the threshold for mandatory government permission before retrenchment from one hundred to three hundred workers, effectively exempting upward of eighty-seven percent of India's industrial establishments from prior scrutiny.<sup>8</sup> The same threshold applies to the requirement to frame certified standing orders, the

---

<sup>6</sup> Ministry of Labour and Employment, Notification S.O. 4805(E) (Nov. 21, 2025) (India); see also Pavan Korada, What Do the Labour Codes Mean for the Indian Worker?, *Progressive Int'l* (Dec. 15, 2025), <https://progressive.international/wire/2025-12-15-what-do-the-labour-codes-mean-for-the-indian-worker/en/>.

<sup>7</sup> Anand Teltumbde, How India's New Labour Codes Dismantle Worker Protections, *Janata Weekly* (Nov. 29, 2025), <https://janataweekly.org/indias-new-labour-codes-assault-on-workers-rights-5-articles/>; Dithi Bhattacharya, New Labour Codes Erase a Century of Hard-Won Workers' Rights in One Stroke, *The Wire* (Dec. 8, 2025), <https://m.thewire.in/article/labour/new-labour-codes-erase-a-century-of-hard-won-workers-rights-in-one-stroke>.

<sup>8</sup> Industrial Relations Code, No. 35 of 2020, § 77 (India) [hereinafter IR Code]; Teltumbde, *supra* note 7 (noting that companies with up to 300 employees may now retrench workers without government approval, covering over 87% of industrial units).

written instrument that historically constrained arbitrary managerial discretion over attendance, discipline, and working conditions.<sup>9</sup> For the vast majority of Indian workers, the rule of law on the factory floor has been rendered optional. Compounding this, fixed-term employment is now permissible across all sectors for perennial work, creating a legally sanctioned framework of permanent insecurity in which workers in constant fear of non-renewal are structurally deterred from asserting any rights, including data rights.<sup>10</sup>

### **Gig and Platform Workers: Recognition Without Substance**

The Code on Social Security, 2020 formally acknowledges gig and platform workers for the first time under Section 2(35), but deliberately declines to classify them as employees.<sup>11</sup> Their social security is premised not on rights but on a welfare fund financed by a cess of one to two percent of aggregator annual turnover, an amount unions describe as a token gesture relative to platform revenues.<sup>12</sup> Section 142 mandates Aadhaar linkage for welfare registration, creating a biometric data pipeline to the state and the aggregator without any accompanying restriction on data use, a point taken up in detail in Part V.<sup>13</sup>

### **Inspection Dilution and Informational Asymmetry**

The OSH Code, 2020 redesignates the Labour Inspector as an "Inspector-cum-Facilitator" whose primary statutory function under Section 51 is to "supply information and advice" to employers rather than to enforce compliance.<sup>14</sup> Inspections are now web-based, algorithm-selected, and subject to advance notice, which critics correctly observe is in tension with ILO Convention No. 81, ratified by India in 1949, which mandates that inspectors be empowered to conduct unannounced visits.<sup>15</sup> The profound irony is that the state now deploys an opaque algorithm to protect employers from scrutiny while leaving workers' own data entirely

---

<sup>9</sup> IR Code § 29 (raising the standing orders threshold from 100 to 300 workers).

<sup>10</sup> Id. § 2(o) (defining "fixed-term employment"); Teltumbde, *supra* note 7 ("The constant fear of non-renewal of their fixed-term contracts will discourage them from exercising their freedom of association.").

<sup>11</sup> Code on Social Security, No. 36 of 2020, § 2(35) (India) [hereinafter CSS].

<sup>12</sup> Id. §§ 114–116; Shirin Akhter, Labour Codes: Structural Rewriting of Workers' Rights, NewsClick (Nov. 29, 2025), <https://www.newslick.in/new-labour-codes-blow-workers-rights> (noting that social security for gig workers remains "aspirational rather than assured" given unspecified contribution rates and unnotified schemes).

<sup>13</sup> CSS § 142.

<sup>14</sup> Occupational Safety, Health and Working Conditions Code, No. 37 of 2020, § 51 (India) [hereinafter OSH Code]; Syed M. Nasif, When Inspection Becomes Advice, Countercurrents.org (Nov. 29, 2025), reprinted in Janata Weekly, <https://janataweekly.org/indias-new-labour-codes-assault-on-workers-rights-5-articles/>.

<sup>15</sup> ILO Convention No. 81 Concerning Labour Inspection in Industry and Commerce art. 12(1)(a), July 19, 1947, 54 U.N.T.S. 3 (ratified by India, Apr. 7, 1949); Nasif, *supra* note 14.

unprotected; the informational asymmetry is not incidental but structural.

Across all four Codes, there is no provision, definition, or rule that speaks to biometric monitoring, GPS tracking, productivity surveillance, algorithmic management, or worker data rights. This silence is the constitutional problem this paper addresses.

### **III. The Architecture of Workplace Surveillance**

The contemporary Indian workplace is not a single site of employment but a distributed network of data-collection points. The proliferation of digital monitoring technologies has produced a layered surveillance architecture in which the employer's informational access to the worker is total, continuous, and largely unchecked by law.

#### **Typology of Monitoring Technologies**

Workplace surveillance in India currently operates across several interconnected vectors: biometric attendance terminals recording fingerprints or iris scans, closed-circuit television systems monitoring shop floors and offices, software tools logging keystrokes, screenshots, and application usage on employer devices, GPS trackers embedded in delivery and logistics applications, and AI-powered productivity-scoring platforms that quantify worker output in real time.<sup>16</sup> Each technology generates a distinct category of personal data; together they construct a granular, continuously updated profile of the worker that the employer controls unilaterally. Remote and hybrid work arrangements, which expanded significantly after 2020, have accelerated the deployment of these tools into workers' homes, extending the surveillance perimeter beyond any defensible workplace boundary.<sup>17</sup>

#### **Biometrics as a Special Category Threat**

Biometric data occupies a qualitatively distinct position within the surveillance architecture because it is immutable. A password can be changed after a breach; a fingerprint cannot. The DPDP Act, 2023 designates biometric data as a subset of personal data but does not create a

---

<sup>16</sup> Workplace Surveillance in a Digital Age, Amlegals (Aug. 5, 2025), <https://amlegals.com/workplace-surveillance-in-a-digital-age/>; Work Place Surveillance and Data Protection: The New Dimension of Labour Rights in Cyber Space, 5 Indian J. L. & Rts. (2025), <https://ijlr.iledu.in/work-place-surveillance-and-data-protection-the-new-dimension-of-labour-rights-in-cyber-space/>.

<sup>17</sup> Legal Implications of Workplace Surveillance in Remote Work, Indian J. L. & Rts. (Apr. 2025), <https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I485.pdf>.

heightened protection regime for it in employment contexts, unlike the EU GDPR, which subjects biometric processing to explicit prohibition absent specific justification.<sup>18</sup> In the gig economy, the Aadhaar-linked biometric registration mandated under Section 142 of the Code on Social Security creates a structural coercion: workers must submit biometric data to access welfare benefits, but no statutory instrument restricts how that data may thereafter be used, aggregated, or shared with platform aggregators.<sup>19</sup>

### **Algorithmic Management and Invisible Discipline**

The most constitutionally significant dimension of contemporary surveillance is not the collection of data but its deployment in automated decision-making. Platform aggregators use algorithmic systems to set task quotas, calculate variable pay, generate performance ratings, and execute deactivations, all without any human deliberation visible to the worker.<sup>20</sup> This constitutes what scholars have termed "algorithmic management": a form of labour control in which the employer's disciplinary function is delegated to an automated system that is simultaneously omnipresent, opaque, and immune from the procedural protections that ordinarily attend workplace discipline.<sup>21</sup> The ILO Code of Practice on Workers' Personal Data (1997) explicitly provides that "decisions concerning a worker should not be based solely on the automated processing of that worker's personal data," yet Indian law contains no equivalent safeguard, statutory or regulatory.<sup>22</sup>

### **The Structural Collapse of Consent**

The consent-based framework that undergirds both the SPDI Rules, 2011 and the DPDP Act, 2023 presupposes a data principal who is free to refuse processing. In employment, that presupposition fails. A worker who declines to consent to GPS monitoring is a worker who

---

<sup>18</sup> DPDP Act § 2(t) (defining personal data to include biometric data); Council Regulation 2016/679, art. 9(1), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]; Employee Monitoring in India, KS&DK (Aug. 29, 2024), <https://ksandk.com/labour-employment/employee-monitoring-privacy-india/>.

<sup>19</sup> CSS § 142; Biometric Privacy in the Gig Economy: Emerging Markets at the Intersection of Identity and Data Rights, SecurePrivacy (May 5, 2025), <https://secureprivacy.ai/blog/gig-economy-biometric-privacy-emerging-markets-india-dpdp>.

<sup>20</sup> Nivedita Majumdar, India's Gig Workers Need a Labour-Sensitive Data Protection Law, The Leaflet (Nov. 17, 2025), <https://theleaflet.in/labour-law/indias-gig-workers-need-a-labour-sensitive-data-protection-law>.

<sup>21</sup> Antonio Aloisi, Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights, 40 Int'l J. Comp. Lab. L. & Indus. Rel. 37, 42 (2024).

<sup>22</sup> ILO, Code of Practice on the Protection of Workers' Personal Data § 5.6 (1997) [hereinafter ILO Code of Practice]; Majumdar, *supra* note 20.

loses the contract; a platform worker who refuses app permissions has no work.<sup>23</sup> The consent is formal but not substantive, and legal frameworks that premise worker protection entirely on consent without addressing the underlying power asymmetry provide, in practice, no protection at all.

#### IV. Constitutional and Pre-DPDP Statutory Framework

The right to privacy in India was decisively constitutionalised in 2017, yet its transformative potential for the workplace remains almost entirely unrealised. The judicial doctrine establishing the right has not, in fifteen years of litigation, been applied by any Indian court to directly restrain private employer surveillance. That gap between constitutional promise and workplace reality is the subject of this Part.

##### The Puttaswamy Framework

In *K.S. Puttaswamy v. Union of India*, the Supreme Court unanimously held that the right to privacy is a fundamental right inhering in Article 21 of the Constitution, encompassing bodily integrity, decisional autonomy, and the protection of personal information.<sup>24</sup> Justice D.Y. Chandrachud, writing for a plurality, held that any state action encroaching on privacy must satisfy a four-part proportionality test: it must be sanctioned by law, pursue a legitimate state aim, be necessary in a democratic society, and be proportionate to the aim pursued in the strict sense.<sup>25</sup> Critically, the Court's reasoning was not confined to state action alone; the plurality judgment expressly contemplated the horizontal application of privacy rights to private actors, noting that the Constitution's transformative vision demands that fundamental rights be capable of protecting individuals against "new forms of surveillance."<sup>26</sup> Employer surveillance has yet to be tested against this framework before any Indian court.

---

<sup>23</sup> Surveillance at Work: Advocating the Right to Not Be Monitored, L. Sch. Pol'y Rev. (Aug. 12, 2025), <https://lawschoolpolicyreview.com/2025/08/12/surveillance-at-work-advocating-the-right-to-not-be-monitored/>; Employee Monitoring Laws in India 2025, MeraMonitor (Nov. 12, 2025), <https://meramonitor.com/employee-monitoring-laws-in-india/>.

<sup>24</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, paras. 78, 119, 180 (India) (per Chandrachud J.).

<sup>25</sup> Id. para. 180 (adopting the proportionality framework from *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353 (India)).

<sup>26</sup> Id. para. 168 ("The right to privacy will necessarily have to abide within its constitutional moorings but it cannot be reduced to a mere abstraction."); see also *Employee Monitoring in India*, KS&DK (Aug. 29, 2024), <https://ksandk.com/labour-employment/employee-monitoring-privacy-india/> (noting that Puttaswamy's proportionality test has not yet been applied to private employer surveillance).

## Kharak Singh and the Professional Sphere

The foundations of a horizontal surveillance doctrine were laid much earlier in *Kharak Singh v. State of Uttar Pradesh*, where the Supreme Court recognised that liberty under Article 21 extended to freedom from physical surveillance of personal movements.<sup>27</sup> While the case arose in the context of state police surveillance, its articulation of the right as encompassing the freedom to carry on one's life, including professional activity, without unreasonable monitoring supplies persuasive precedent for restraining private employer surveillance.<sup>28</sup>

## The IT Act, 2000 and SPDI Rules, 2011

Before the DPDP Act, the only statutory instruments offering any protection to worker data were Section 43A of the Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Section 43A imposes a civil liability on body corporates that negligently handle sensitive personal data or information ("SPDI"), while the SPDI Rules, 2011 define SPDI to include biometric data and passwords, and require a privacy policy, written consent, and purpose limitation.<sup>29</sup> However, the Rules contain two structural weaknesses in the employment context. First, they apply only to body corporates and not to individuals or unregistered enterprises, excluding a large segment of Indian employers. Second, the definition of SPDI does not encompass GPS location trails, productivity metrics, keystroke logs, or behavioural scores generated by monitoring software, meaning the most pervasive forms of contemporary workplace surveillance fall entirely outside the Rules' scope.<sup>30</sup>

## Doctrinal Gap: No Enforcement Mechanism

Even where the IT Act framework technically applies, no worker has successfully invoked Section 43A to restrain or remedy employer surveillance, because the provision is civilly

---

<sup>27</sup> *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295, para. 20 (India).

<sup>28</sup> Surveillance at Work: Advocating the Right to Not Be Monitored, L. Sch. Pol'y Rev. (Aug. 12, 2025), <https://lawschoolpolicyreview.com/2025/08/12/surveillance-at-work-advocating-the-right-to-not-be-monitored/>.

<sup>29</sup> Information Technology Act, No. 21 of 2000, § 43A (India) [hereinafter IT Act]; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rr. 3, 5, G.S.R. 313(E) (India) [hereinafter SPDI Rules].

<sup>30</sup> SPDI Rules r. 3 (limiting SPDI to passwords, financial information, health data, sexual orientation, biometric data, and medical records; omitting location data, productivity metrics, and behavioural logs); see Work Place Surveillance and Data Protection: The New Dimension of Labour Rights in Cyber Space, 5 Indian J. L. & Rts. (2025), <https://ijlr.iledu.in/work-place-surveillance-and-data-protection-the-new-dimension-of-labour-rights-in-cyber-space/>.

framed and requires proof of wrongful loss or gain, a standard that is difficult to satisfy in cases of systemic, ongoing data collection where harm is diffuse and prospective.<sup>31</sup> The SPDI Rules further permit processing on the basis of the worker's "consent" as embodied in the employment contract itself, replicating in statutory form the same consent fiction identified in Part III. The combined effect is a statutory architecture that formally acknowledges worker data rights but operationally provides no remedy, leaving the constitutional mandate of Puttaswamy without a legislative mechanism through which it may be vindicated in the workplace.

## **V. The DPDP Act, 2023: Promise, Ambiguity, and Structural Limits in Employment**

The Digital Personal Data Protection Act, 2023 is the most comprehensive privacy legislation India has enacted, and its entry into force represents a structurally important development for worker data rights. The Act displaces the fragmented SPDI framework and introduces a principled regime of rights, obligations, and redressal. Yet a careful reading of its text alongside the employment context reveals that its promise is significantly qualified by definitional silences, a critical consent exception, and the complete absence of any provision on automated decision-making.

### **Employer as Data Fiduciary: The Rights Architecture**

The Act classifies employers as "Data Fiduciaries" under Section 2(i), imposing obligations under Section 8 to ensure data accuracy, implement security safeguards, and delete personal data once it is no longer necessary for the stated purpose.<sup>32</sup> Workers, as "Data Principals" under Section 2(j), acquire the right under Section 11 to obtain a summary of their processed personal data and the identities of Data Fiduciaries to whom their data has been disclosed, and under Section 12 the right to correction and erasure.<sup>33</sup> These provisions mark a genuine doctrinal advance: for the first time, Indian law recognises the worker as a rights-bearing subject in relation to employer data processing rather than a passive object of managerial discretion.

---

<sup>31</sup> IT Act § 43A (conditioning liability on "wrongful loss or wrongful gain"); Employee Monitoring Laws in India 2025, MeraMonitor (Nov. 12, 2025), <https://meramonitor.com/employee-monitoring-laws-in-india/>.

<sup>32</sup> DPDP Act §§ 2(i), 8.

<sup>33</sup> Id. §§ 2(j), 11–12; see Impact of the Digital Personal Data Protection Act on Employee Data in India, ACC Resource Library (Sept. 23, 2025), <https://www.acc.com/resource-library/impact-digital-personal-data-protection-act-employee-data-india>.

## The Section 7 Exception and the Consent Fiction

Section 7 of the DPDP Act permits processing of personal data for "legitimate uses" without obtaining the Data Principal's consent, including processing "for the purposes of employment."<sup>34</sup> This exception is the Act's most consequential structural flaw in the labour context. By authorising processing for employment purposes without requiring consent, the provision ratifies precisely the power asymmetry that makes consent in employment relationships illusory. An employer may collect GPS data, productivity logs, and behavioural scores under the shelter of Section 7 without any obligation to specify purpose, obtain agreement, or justify proportionality.<sup>35</sup> The provision effectively reproduces the consent fiction of the SPDI Rules in a more sophisticated statutory form: the worker is nominally a rights-bearing Data Principal, but the most routine processing of their data requires no engagement with those rights at all.

## Definitional Silences and Gig Workers

The Act does not define "employee," "employer," or "employment relationship."<sup>36</sup> This omission has acute consequences for gig and platform workers, who are, as noted in Part II, deliberately excluded from the employee category under the Labour Codes. A platform aggregator can credibly argue that the relationship with a gig worker is one of service provision rather than employment, placing data processing under the Act's general commercial framework rather than any employment-specific norm.<sup>37</sup> The Act is similarly silent on data collected during pre-employment screening, post-termination retention, and the monitoring of interns and trainees, creating further regulatory lacunae at the margins of the employment relationship.

---

<sup>34</sup> DPDP Act § 7(f).

<sup>35</sup> Id.; India's Data Privacy Law Loopholes: Are YOUR Workplace Rights Protected?, Whalesbook (Dec. 11, 2025), <https://www.whalesbook.com/news/English/tech/> (noting that Section 7 "effectively immunises routine employer surveillance from the consent architecture").

<sup>36</sup> See Digital Personal Data Protection Act, 2023: A Ready Reckoner for Employers, SCC Online Blog (Nov. 10, 2024), <https://www.sconline.com/blog/post/2024/11/11/digital-personal-data-protection-act-2023-employers-guide/> (observing that the Act "does not define the employment relationship or prescribe sector-specific obligations for employers").

<sup>37</sup> Nivedita Majumdar, India's Gig Workers Need a Labour-Sensitive Data Protection Law, The Leaflet (Nov. 17, 2025), <https://theleaflet.in/labour-law/indias-gig-workers-need-a-labour-sensitive-data-protection-law> (arguing that the DPDP Act's failure to cover non-standard work relationships "replicates and deepens the statutory exclusion in the Labour Codes").

## The Automated Decision-Making Gap

The most critical absence in the DPDP Act relative to the needs of monitored workers is the complete lack of any provision restricting solely automated decision-making. The EU General Data Protection Regulation, Article 22, provides data subjects with the right not to be subject to decisions based solely on automated processing that produce significant effects, including termination.<sup>38</sup> Aloisi, in a 2024 analysis of algorithmic management under European law, demonstrates that this provision, read alongside Article 88's authorisation of member state employment-specific rules, creates a genuine bulwark against the worst excesses of platform discipline.<sup>39</sup> The DPDP Act contains no analogous provision. An Indian platform worker deactivated by an algorithm has no statutory right to demand human review, no right to know which data triggered the decision, and no right to challenge the automated outcome before the Data Protection Board.<sup>40</sup> Section 13's right to nominate a grievance representative and Section 14's right to approach the Data Protection Board are procedural rather than substantive: they provide a forum but not a cause of action for algorithmic harm.<sup>41</sup>

## VI. Precarious Workers at the Intersection: Gig, Platform, and Contract Labour

The structural failures identified in the preceding Parts do not fall equally across the workforce. Gig, platform, and fixed-term contract workers bear a disproportionate share of the legal deficit because they are the most intensively monitored workers in the Indian economy and simultaneously the least protected by either the Labour Codes or the DPDP Act. Their situation represents not an oversight in the legislative design but its logical endpoint.

### Platform Surveillance as the Primary Mechanism of Labour Control

For platform workers employed by aggregators operating in logistics, food delivery, ride-hailing, and domestic services, surveillance is not incidental to the work relationship but constitutive of it. Continuous GPS tracking determines task allocation; algorithmic rating scores determine earnings and access to premium orders; automated deactivation replaces the procedurally governed termination that the Industrial Relations Code affords to formal

---

<sup>38</sup> GDPR, *supra* note 18, art. 22(1).

<sup>39</sup> Aloisi, *supra* note 21, at 51–55.

<sup>40</sup> See HR and the Digital Personal Data Protection Act, 2023, LinkedIn Pulse (Aug. 23, 2025), <https://www.linkedin.com/pulse/hr-digital-personal-data-protection-act-2023-dpdp-era-murugan-wiarf> (noting that the DPDP Act does not impose any requirement for human oversight of automated employment decisions).

<sup>41</sup> DPDP Act §§ 13–14.

employees.<sup>42</sup> Unlike a factory worker whose conditions of work are, in principle, subject to the OSH Code's schedule of rights, a platform worker's entire working existence is mediated by an algorithmic system that is privately designed, opaquely operated, and wholly outside the inspection framework of any Labour Code.<sup>43</sup> The Karnataka Platform-Based Gig Workers (Social Security and Welfare) Act, 2024 represents the most significant legislative response to this gap at the state level, mandating disclosure of the criteria used in rating systems, the parameters of automated monitoring, and the grounds for deactivation.<sup>44</sup> However, its definitional scope is limited to systems operating substantially by automated means, a formulation that aggregators operating hybrid human-algorithmic review systems may exploit to escape coverage.<sup>45</sup>

### **The Aadhaar-Surveillance Convergence**

Section 142 of the Code on Social Security mandates Aadhaar-based registration for gig workers seeking access to welfare fund benefits, creating a biometric data pipeline that is simultaneously a condition of state welfare access and a source of commercial data for aggregators.<sup>46</sup> No provision in the CSS, the DPDP Act, or the Aadhaar Act, 2016 expressly restricts the use of Aadhaar-linked data by private aggregators beyond authentication, meaning the worker's biometric identity, once submitted for welfare registration, enters a data ecosystem with no legally mandated use limitations.<sup>47</sup> This Aadhaar-surveillance convergence is particularly acute because it is the state that compels biometric disclosure and the aggregator that benefits from it, creating a triangular power structure in which the worker is entirely without leverage.

---

<sup>42</sup> Majumdar, *supra* note 20; Gig Workers Under Social Security Code, Corrida Legal (Nov. 21, 2025), <https://corridalegal.com/gig-workers-under-social-security-code-employer-obligations-benefits-legal-framework-in-india/>.

<sup>43</sup> See India: Karnataka's Gig Worker Law Introduces Algorithmic Transparency but Enforcement Remains Unclear, Bus. & Hum. Rts. Resource Ctr. (Aug. 20, 2025), <https://www.business-humanrights.org/en/latest-news/india-karnatakas-gig-worker-law-introduces-algorithmic-transparency-but-enfo>.

<sup>44</sup> Karnataka Platform-Based Gig Workers (Social Security and Welfare) Act, 2024 (India); see The Draft Karnataka Platform-Based Gig Workers Social Security and Welfare Bill, 2024, PRS India (Feb. 24, 2026), <https://prsindia.org/bills/states/the-draft-karnataka-platform-based-gig-workers-social-security-and-welfare-bill-2024>.

<sup>45</sup> Bus. & Hum. Rts. Resource Ctr., *supra* note 43 (identifying the "automated means" definitional loophole as a significant enforcement vulnerability).

<sup>46</sup> CSS § 142; Biometric Privacy in the Gig Economy: Emerging Markets at the Intersection of Identity and Data Rights, SecurePrivacy (May 5, 2025), <https://secureprivacy.ai/blog/gig-economy-biometric-privacy-emerging-markets-india-dpdp>.

<sup>47</sup> Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, §§ 29, 33 (India) (restricting sharing of identity information but not use of data derived from authentication).

## Algorithmic Deactivation Without Recourse

The Telangana Gig and Platform Workers (Registration, Social Security and Welfare) Act, 2025 takes a stronger position, prohibiting arbitrary deactivation and mandating a minimum seven-day notice period alongside a written statement of reasons before any termination.<sup>48</sup> The contrast between the Telangana framework and the central Labour Codes illustrates a deepening regulatory fracture: state legislatures are beginning to fill the rights gap that the central Codes created, generating a patchwork of protections whose coverage depends on the state in which a worker happens to be registered rather than any uniform national standard.<sup>49</sup> For the majority of India's estimated fifteen million gig workers who operate across state lines, this jurisdictional fragmentation compounds rather than resolves the fundamental problem.<sup>50</sup>

## The Consent Problem Restated

Platform terms of service constitute the contractual instrument through which aggregators extract consent to comprehensive data collection. These instruments are drafted unilaterally, presented on a take-it-or-leave-it basis, and frequently updated without individualised notice.<sup>51</sup> The ILO Code of Practice on Workers' Personal Data provides that "workers should not be compelled by means of undue pressure or threat to waive their right to privacy," but no Indian statute operationalises this principle as an enforceable right against platform aggregators.<sup>52</sup> The consent architecture of the DPDP Act cannot salvage this position: where the choice is between accepting comprehensive surveillance and having no income, consent in any meaningful legal sense is absent.

## VII. Comparative Framework: Lessons from the EU and the ILO

No jurisdiction has fully resolved the tension between employer surveillance and worker privacy, but two external frameworks offer normatively principled and practically workable

---

<sup>48</sup> Majumdar, *supra* note 20 (describing the Telangana Gig and Platform Workers Act, 2025 as prohibiting arbitrary deactivation and mandating seven-day advance notice with written reasons).

<sup>49</sup> See Anvita Singh, Do India's Labour Codes Address Informal Workers' Needs?, IDR Online (Apr. 7, 2025), <https://idronline.org/article/rights/do-indias-labour-codes-address-informal-workers-needs/> (documenting the growing divergence between state-level gig worker protections and the central Labour Codes framework).

<sup>50</sup> India's New Labor Codes Extend Social Security Coverage to Gig Workers, Fisher Phillips (Jan. 4, 2026), <https://www.fisherphillips.com/en/news-insights/indias-new-labor-codes-extend-social-security-coverage-to-gig-workers.html> (estimating India's platform workforce at approximately fifteen million workers).

<sup>51</sup> Majumdar, *supra* note 20.

<sup>52</sup> ILO Code of Practice, *supra* note 22, § 5.2.

models against which the Indian legislative deficit may be benchmarked. The EU's General Data Protection Regulation and the ILO Code of Practice on Workers' Personal Data together constitute the most developed international architecture for worker data rights, and their doctrinal contributions are directly translatable into the Indian constitutional and statutory context.

### **The ILO Code of Practice: A Principled Minimum**

The ILO Code of Practice on Workers' Personal Data (1997) predates digital platform work, yet its foundational principles address the core problems identified in this paper with considerable precision. The Code establishes that worker data should be collected only for purposes "directly relevant to the employment relationship," prohibits collection on the basis of workers' trade union membership or political opinions, and provides in Article 5.6 that decisions affecting a worker must not be based solely on the automated processing of their personal data.<sup>53</sup> It further requires employers to inform workers of any monitoring systems in operation, specifying the nature of the data collected, the purposes for which it is used, and the persons to whom it may be disclosed.<sup>54</sup> India has not ratified ILO Convention No. 108 on data protection, and the Code itself is non-binding. However, it constitutes persuasive interpretive authority of considerable weight: the Supreme Court in *Puttaswamy* drew extensively on international instruments to substantiate the content of the fundamental right to privacy, and the ILO Code supplies the labour-specific content that *Puttaswamy*'s proportionality doctrine requires but does not itself articulate.<sup>55</sup>

### **The GDPR Framework: Algorithmic Accountability in Employment**

The EU General Data Protection Regulation represents the most sophisticated statutory response to workplace surveillance currently in operation. Three provisions are of particular relevance to the Indian context. Article 22 grants data subjects the right not to be subject to decisions based solely on automated processing that produce significant legal or similarly significant effects, and requires that where such processing occurs, the controller must

---

<sup>53</sup> ILO Code of Practice, *supra* note 22, §§ 5.1, 5.6, 6.1.

<sup>54</sup> *Id.* § 11.1 ("Workers should be informed in advance of any electronic monitoring systems used in the workplace, the data collected, the purpose for which they are used, and the period of retention.").

<sup>55</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, paras. 63, 115, 168 (India) (drawing on the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and comparative constitutional jurisprudence to substantiate the content of the fundamental right to privacy).

implement suitable safeguards including the right to obtain human intervention, express a point of view, and contest the decision.<sup>56</sup> Article 88 authorises member states to adopt more specific rules ensuring the protection of the rights and freedoms of employees in the context of the processing of personal data in employment, covering collection at recruitment, performance monitoring, and termination, provided those rules include suitable and specific measures to safeguard the data subjects' human dignity, legitimate interests, and fundamental rights.<sup>57</sup> Article 9 prohibits the processing of biometric data for the purpose of uniquely identifying a natural person unless specific, enumerated exceptions apply, none of which covers routine employer convenience.<sup>58</sup>

Aloisi's 2024 analysis of algorithmic management under GDPR demonstrates that Articles 22 and 88, read together with non-discrimination law and collective rights instruments, create a normative framework capable of "rebalancing the informational asymmetries that are structurally constitutive of platform work."<sup>59</sup> Critically, Aloisi identifies the combination of individual data rights and collective transparency obligations as indispensable: individual rights are too costly to assert in isolation, but collective transparency obligations imposed on the employer create systemic accountability that benefits the entire workforce.<sup>60</sup>

### **The EU Platform Work Directive, 2024**

The EU Directive on Platform Work, adopted in 2024, operationalises these principles specifically for the gig economy. The Directive creates a rebuttable presumption of employment for platform workers, mandates algorithmic transparency by requiring platforms to disclose to workers and their representatives the parameters of automated monitoring and decision-making systems, prohibits automated deactivation without human review, and requires that any disciplinary measure resulting from automated processing be subject to human oversight before implementation.<sup>61</sup> The Directive's presumption of employment is particularly instructive for India, where the Code on Social Security's deliberate non-

---

<sup>56</sup> GDPR, *supra* note 18, art. 22(1), (3).

<sup>57</sup> *Id.* art. 88(1), (2).

<sup>58</sup> *Id.* art. 9(1).

<sup>59</sup> Aloisi, *supra* note 21, at 55.

<sup>60</sup> *Id.* at 61–63 (arguing that "the individual rights model is structurally inadequate for workplace contexts and must be supplemented by collective information and consultation rights vested in trade unions and works councils").

<sup>61</sup> Directive 2024/2831 of the European Parliament and of the Council on Improving Working Conditions in Platform Work, arts. 9–12, 2024 O.J. (L 2831) 1 (EU); see also Cynthia Estlund & Seth Harris, Algorithmic Management and a New Generation of Rights at Work, 69 N.Y.U. Ann. Surv. Am. L. 385, 402 (2025).

classification of gig workers as employees is the root cause of both their social security deficit and their data rights deficit simultaneously.

### **Lessons for Indian Reform**

Three specific transplantable principles emerge from this comparative survey. First, purpose limitation must be defined by statute with reference to employment necessity rather than left to employer discretion or contractual terms. Second, a right against solely automated decision-making affecting workers must be enacted as a substantive statutory right, not merely a procedural grievance mechanism. Third, transparency obligations must be collective as well as individual, requiring employers to disclose monitoring systems to worker representatives rather than only to individual data principals who lack the resources or job security to exercise rights in isolation.<sup>62</sup> Absent these three elements, any Indian reform will replicate the structural inadequacy of the DPDP Act's current framework.

### **VIII. A Draft Model Clause for Worker Data Protection**

The doctrinal and comparative analysis in the preceding Parts converges on a single legislative conclusion: incremental judicial interpretation of Puttaswamy cannot substitute for targeted statutory reform. The model clause below is designed as a concrete legislative contribution. It may be operationalised in three distinct ways: as a worker-specific rule notified under Section 40 of the DPDP Act, 2023, empowering the Central Government to prescribe additional obligations for specified classes of Data Fiduciaries; as a mandatory provision inserted into standing orders framed under the Industrial Relations Code, 2020; or as a contractual minimum imposed on platform aggregators as a condition of registration under the Code on Social Security, 2020.<sup>63</sup> The clause draws its normative architecture from the ILO Code of Practice (1997), the GDPR Articles 22 and 88, the EU Platform Work Directive (2024), and the proportionality standard of Puttaswamy, translating each into an enforceable domestic instrument.<sup>64</sup>

---

<sup>62</sup> Aloisi, *supra* note 21, at 65–67; ILO Code of Practice, *supra* note 22, § 12 (specifying collective rights of worker representatives to be informed of monitoring systems).

<sup>63</sup> DPDP Act § 40 (empowering the Central Government to notify additional obligations for significant and specified Data Fiduciaries); IR Code § 29 (standing orders framework); CSS §§ 114–116 (aggregator registration and welfare fund obligations).

<sup>64</sup> ILO Code of Practice, *supra* note 22, §§ 5.1, 5.6, 11.1; GDPR, *supra* note 18, arts. 22, 88; Directive 2024/2831, *supra* note 61, arts. 9–12; K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, para. 180 (India).

**Model Clause X:** Protection of Worker Personal Data and Regulation of Workplace Surveillance.

**X.1 Definitions.** For the purposes of this Clause:

(a) "Worker" means any person engaged in employment, fixed-term contract, apprenticeship, consultancy, or platform-based engagement with an employer or aggregator, regardless of classification under the Labour Codes.

(b) "Worker data" means any personal data, biometric data, location data, productivity metrics, behavioural scores, performance ratings, communication records, or any other data generated, collected, or inferred in connection with the engagement of a worker, whether by automated or manual means.

(c) "Automated decision" means any decision producing a significant effect on a worker's engagement, earnings, task allocation, rating, discipline, or deactivation, arrived at without meaningful human deliberation.

(d) "Aggregator" shall have the meaning assigned under Section 2(1) of the Code on Social Security, 2020.<sup>65</sup>

**X.2 Purpose Limitation.** An employer or aggregator shall collect and process worker data only for purposes that are directly and demonstrably necessary for the performance of the work engagement. Processing for purposes of trade union surveillance, political opinion monitoring, or personal conduct outside working hours is absolutely prohibited, and no contractual term or consent shall authorise such processing.<sup>66</sup>

**X.3 Prior Transparency Notice.** Before deploying any monitoring system, the employer or aggregator shall provide each worker with a written Surveillance Disclosure Notice specifying:

(a) the nature and categories of worker data to be collected;

(b) the specific purpose for which each category is processed and the legal basis relied upon;

---

<sup>65</sup> CSS § 2(1)(a); cf. IR Code § 2(o) (definition of fixed-term employment).

<sup>66</sup> ILO Code of Practice, *supra* note 22, §§ 6.1, 6.5; GDPR, *supra* note 18, art. 9(1) (prohibiting processing of special category data absent specific justification).

(c) whether automated decision-making is applied, and if so, the logic, parameters, and weight assigned to data inputs;

(d) the retention period for each category of data; and

(e) the identities of all third-party processors to whom data may be disclosed.

The Notice shall be provided in plain language in the worker's preferred language, shall not be embedded within a general terms of service, and shall require a separately documented acknowledgment distinct from the work contract.<sup>67</sup>

**X.4 Right Against Solely Automated Decisions.** No disciplinary measure, wage deduction, task withdrawal, rating alteration, suspension, or deactivation shall be based solely on the automated processing of worker data. Every such decision shall:

(a) be reviewed by a designated human officer before implementation;

(b) be accompanied by a written statement of reasons identifying the specific data relied upon and the criteria applied; and

(c) be subject to a worker's right of representation before a final decision is taken.

The burden of demonstrating that a human review was conducted shall rest on the employer or aggregator.<sup>68</sup>

**X.5 Biometric Data Restriction.** Collection, storage, and processing of biometric data shall be permitted only for purposes of authentication mandated by statute. Biometric data shall not be used for performance evaluation, productivity scoring, or disciplinary purposes, and shall not be transferred to any third party, including platform aggregators, beyond what is strictly necessary for authentication. Biometric data shall be deleted within thirty days of the conclusion of the work engagement.<sup>69</sup>

---

<sup>67</sup> ILO Code of Practice, *supra* note 22, § 11.1; Directive 2024/2831, *supra* note 61, art. 9(2) (requiring platforms to inform workers of monitoring systems in plain and intelligible language, separately from general contractual terms).

<sup>68</sup> GDPR, *supra* note 18, art. 22(3); Directive 2024/2831, *supra* note 61, art. 10(1) (prohibiting deactivation through solely automated decision-making without human review); Aloisi, *supra* note 21, at 55–58.

<sup>69</sup> Cf. SPDI Rules, *supra* note 29, r. 7 (mandating deletion of sensitive personal data once the purpose is served); SecurePrivacy, *supra* note 19.

**X.6 Worker Data Rights.** Every worker shall have the right, exercisable free of charge and within fifteen working days of a written request:

- (a) to obtain a complete record of all worker data held by the employer or aggregator, including derived scores and inferred attributes;
- (b) to correct factually inaccurate data;
- (c) to request deletion of data no longer necessary for the stated purpose; and
- (d) to receive a human-intelligible explanation of any automated decision that has produced a significant effect on their engagement.<sup>70</sup>

**X.7 Collective Transparency.** Where a workplace has a recognised trade union, works committee, or worker representative body, the employer or aggregator shall disclose to that body, at intervals not exceeding six months, a written report on all monitoring systems deployed, the categories of data collected, and any changes to automated decision-making parameters introduced during the reporting period.<sup>71</sup>

**X.8 Data Protection Officer.** Every employer or aggregator engaging fifty or more workers shall designate a Worker Data Protection Officer responsible for ensuring compliance with this Clause. The Officer shall be accessible to workers, shall maintain a register of all monitoring systems, and shall handle worker data grievances with a binding resolution within thirty days, subject to appeal to the Data Protection Board established under the DPDP Act, 2023.<sup>72</sup>

**X.9 Non-Derogation.** No provision of any work contract, platform terms of service, or standing order shall exclude or limit the rights conferred under this Clause. Any such provision shall be void to the extent of the inconsistency.<sup>73</sup>

---

<sup>70</sup> DPDP Act §§ 11–12; GDPR, *supra* note 18, art. 15 (right of access), art. 22(3) (right to human intervention and explanation in automated decisions).

<sup>71</sup> Aloisi, *supra* note 21, at 61–65; ILO Code of Practice, *supra* note 22, § 12 (collective rights of worker representatives to be informed of monitoring systems); Directive 2024/2831, *supra* note 61, art. 9(3) (disclosure obligation to worker representatives).

<sup>72</sup> DPDP Act § 14 (Data Protection Board); cf. GDPR, *supra* note 18, art. 37 (mandatory Data Protection Officer for large-scale processing of personal data).

<sup>73</sup> Cf. IR Code § 13 (nullity of standing order provisions inconsistent with the Code); see also Majumdar, *supra* note 20 (emphasising the need for non-derogable worker data rights that cannot be contracted away through platform terms of service).

## IX. Conclusion

The argument of this paper can be stated simply: the Labour Codes of 2020 created a legislative framework that is structurally blind to the most consequential site of power over workers in the contemporary Indian economy, namely, the employer's informational dominance over the worker through continuous digital surveillance. That blindness is not remedied by the DPDP Act, 2023, whose consent architecture is defeated by employment power asymmetry, whose Section 7 exception immunises routine employer data processing, and whose silence on automated decision-making leaves the algorithmically disciplined worker without a cause of action.

The constitutional deficit is stark. Puttaswamy holds that any encroachment on informational privacy must satisfy the requirements of legality, legitimate aim, necessity, and proportionality.<sup>74</sup> Employer surveillance as currently practiced satisfies none of these requirements in a legally verifiable sense: it is conducted without statutory authorisation, for purposes defined unilaterally by the employer, to an extent unrestricted by any necessity principle, and through mechanisms whose proportionality has never been judicially examined.<sup>75</sup> The Constitution demands more, and the legislature has not yet delivered it.

The paper has identified three axes of necessary reform. First, worker-specific rules must be notified under Section 40 of the DPDP Act, explicitly covering gig and platform workers and closing the definitional gap created by the Labour Codes' non-classification of platform labour.<sup>76</sup> Second, a statutory right against solely automated decisions affecting workers must be enacted, drawing on the normative architecture of GDPR Article 22 and the EU Platform Work Directive's human review mandate.<sup>77</sup> Third, the ILO Code of Practice's principle of employment-necessity as the ceiling of legitimate data collection must be incorporated as a non-derogable statutory standard, immune to contractual displacement through platform terms

---

<sup>74</sup> K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, para. 180 (India).

<sup>75</sup> See Employee Monitoring in India, KS&DK (Aug. 29, 2024), <https://ksandk.com/labour-employment/employee-monitoring-privacy-india/> (observing that the proportionality of employer surveillance "has never been subjected to constitutional scrutiny before an Indian court").

<sup>76</sup> DPDP Act § 40; Nivedita Majumdar, India's Gig Workers Need a Labour-Sensitive Data Protection Law, The Leaflet (Nov. 17, 2025), <https://theleaflet.in/labour-law/indias-gig-workers-need-a-labour-sensitive-data-protection-law>.

<sup>77</sup> GDPR, *supra* note 18, art. 22; Directive 2024/2831, *supra* note 61, art. 10(1); Antonio Aloisi, Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights, 40 Int'l J. Comp. Lab. L. & Indus. Rel. 37, 65 (2024).

of service.<sup>78</sup>

The model clause proposed in Part VIII operationalises all three axes within the existing statutory framework without requiring comprehensive new legislation, demonstrating that the reform is feasible and immediate. The deeper aspiration, however, is constitutional. A legal order that permits the continuous, opaque, automated surveillance of its most precarious workers while providing them no statutory recourse has not merely failed its labour policy; it has failed the transformative promise of a Constitution that places dignity at the centre of the fundamental rights chapter.<sup>79</sup> Restoring that promise in the digitised workplace is not a regulatory refinement; it is a constitutional obligation.

---

<sup>78</sup> ILO Code of Practice on the Protection of Workers' Personal Data § 5.1 (1997); see Surveillance at Work: Advocating the Right to Not Be Monitored, L. Sch. Pol'y Rev. (Aug. 12, 2025), <https://lawschoolpolicyreview.com/2025/08/12/surveillance-at-work-advocating-the-right-to-not-be-monitored/>.

<sup>79</sup> See Dithhi Bhattacharya, New Labour Codes Erase a Century of Hard-Won Workers' Rights in One Stroke, The Wire (Dec. 8, 2025), <https://m.thewire.in/article/labour/new-labour-codes-erase-a-century-of-hard-won-workers-rights-in-one-stroke> (framing the Labour Codes as a regression from the Constitution's original vision of worker dignity and social justice embedded in Articles 38, 39, and 43 of the Directive Principles of State Policy).