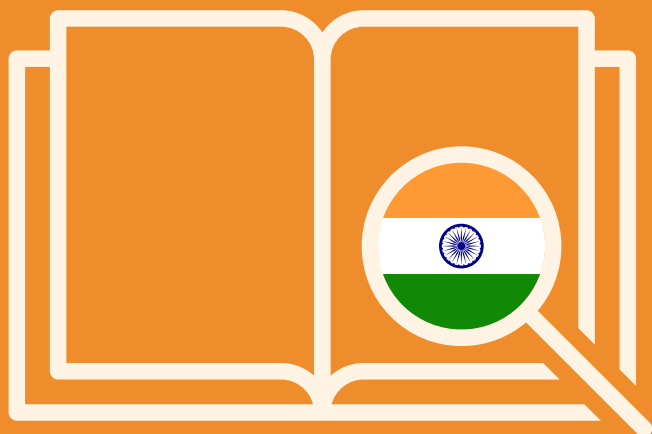


Deepa Padmar and Alok Prasanna Kumar
June 2026

Negotiating Digitalised Workplaces

Rights and Obligations, India



Imprint

Publisher

Friedrich-Ebert-Stiftung e.V.
Godesberger Allee 149
53175 Bonn
Germany
info@fes.de

Publishing department

Division for International Cooperation |
Global and European Policy

Responsibility for content and editing

Mirko Herberg, Director, Global Trade Union Project

Contact

Blanka Balfer
blanka.balfer@fes.de

Design/Layout

pertext | corporate publishing
www.pertext.de

The views expressed in this publication are not necessarily those of the Friedrich-Ebert-Stiftung e.V. (FES). Commercial use of the media published by the FES is not permitted without the written consent of the FES. FES publications may not be used for election campaign purposes.

June 2026

© Friedrich-Ebert-Stiftung e.V.

ISBN 978-3-98628-891-4

Further publications of the Friedrich-Ebert-Stiftung can be found here:

➤ www.fes.de/publikationen

Deepa Padmar and Alok Prasanna Kumar
June 2026

Negotiating Digitalised Workplaces

Rights and Obligations, India

Contents

Foreword	3
1. Introduction – Technology at Work Is a Labour Issue	4
2. Examples of Digital Technologies Used at Workplaces in India	7
3. What Are Your Rights – And What Are Management’s Obligations?	9
Information Technology Act, 2000 (“IT Act”) & the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (“SPDI Rules”)	9
Digital Data Protection Act, 2023 (“DPDP Act”)	11
Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (“the POSH Act”)	13
Rights of Persons with Disabilities Act, 2016 (“the RPWD Act”)	14
Labour Codes.	14
Code on Wages, 2019 (“the Wage Code”)	14
Industrial Relations Code, 2020/39 (“the IR Code”)	14
Social Security Code (“the SS Code”)	15
Occupational Safety, Health and Working Conditions Code.	16
Shops and Establishments Laws	16
Laws governing Platform-based gig work.	16
Constitution of India: Article 21/Judicial Precedents.	18
4. The Checklists of Questions You Have a Right to Ask!	19
5. Filling the Gaps – Bargaining Topic Suggestions	23
6. Summary Reflections	25
7. Annex – Links to the Laws Covered	26
8. Glossary List	27

Foreword

Across the world, management in both the public and private sectors is deploying digital technologies with the aim of improving productivity and efficiency. Such technologies have a direct impact on working conditions and workers' rights. Jobs are being (semi-)automated, new competencies are required and work and workers are becoming quantified as their actions and non-actions are turned into data points and analysed through algorithmic systems. The negative impact of these systems on workers is well documented.

Yet anecdotal evidence from multiple countries suggests that shop stewards and Occupational Health and Safety representatives to a large degree are not discussing the use of digital technologies with management. The representatives mention that they feel they lack knowledge about the particularities of digital technologies and why they should pay careful attention to them. Many report that management never raises the issues of digitalisation with them, nor do they feel they have a sound overview of how to apply existing laws and agreements to spur these discussions.

Although some unions are successfully negotiating contract language about the digitalisation of work as evidenced by PSI's Digital Bargaining Hub, the vast majority are still not. To support unions in their negotiations with management, this series of reports brings to light what rights workers have when digital systems are deployed at work and what obligations management have in relation to the workers. The reports provide ready-to-use checklists of questions, and collective bargaining suggestions to bridge legal gaps.

The Friedrich-Ebert-Stiftung realises that technology deployment without workers involvement not only subjects workers to control but also changes the balance of power at the workplace in favour of employers. Workers may feel increasingly alienated and objectified. We have understood that an unprotected and disempowered workforce is not only less productive but tends to lose trust in the promises and institutions that are supposed to guarantee decent work and a decent live. Therefore, contributing to workers'

capacity to claim their rights and negotiate working conditions in a digitalised workplace is a service to democracy and justice. This is what this project aims to achieve – by making transparent what institutional power, i.e. rights, laws and labour market agreements workers have at their disposal. We hope that the case studies presented will lead to a more thorough and strategic response by workers and organised labour in the countries studied and to more countries embarking on the path towards negotiated introduction and use of digital technologies.

We owe Christina J. Colclough, Director of The Why Not Lab, Denmark, our gratitude for providing the initial spark for this project and for being an enthusiastic and competent mentor to the case study authors. Her relentless dedication to challenge, motivate and capacity build the labour movement to build power in the digital economy is unparalleled and has been the inspiration behind many collaborative undertakings of the FES Global and national Trade Union Projects.

We thank the authors of the country studies for their professionalism and enthusiasm to explore uncharted territory, for the discoveries of potential leverage points and for their "thinking forward" to take the next steps in building workers' power.

Finally, Blanka Balfer, FES, deserves praise for being the silent backbone of this project (and so many others) that allow FES to use its global network for the benefit of the global labour movement.

May this series of reports serve as a stepping stone for deeper engagement, collective bargaining and policy-making and policy-enforcing success in the digital economy of today and tomorrow!

Mirko Herberg

*Director, Global Trade Union Project
Friedrich-Ebert-Stiftung*

1.

Introduction – Technology at Work Is a Labour Issue

You may already be working with digital technologies without having been asked about them.

An app to clock in. Software that scores your calls. Dashboards measuring performance. GPS tracking in vehicles. AI screening job applications. Cameras in new places.

These technologies are often presented as technical tools to improve efficiency or service quality. But for workers, they change how work is organised, monitored, evaluated, and controlled.

This report is designed to help workers and unions understand which laws already apply, which questions they have a right to ask based on those laws, and how to use those rights when digital technologies are introduced or used at work. It also shows how collective bargaining can be used to address gaps that existing law does not fully regulate.

Digital technologies are no longer peripheral tools in the workplace. Across the world, they increasingly sit at the centre of managerial power, shaping how work is organised, paced, evaluated and controlled. Biometric attendance systems, GPS tracking, algorithmic task allocation, AI-based recruitment tools, performance dashboards and automated decision-making systems are being rolled out across sectors with little warning and, too often, without meaningful consultation with workers or their trade unions.

For workers and union officials, this transformation raises a fundamental question: who controls technology at work, and in whose interests is it deployed? While employers routinely present digitalisation as neutral, inevitable or purely technical, workers experience it as a restructuring of power relations. Digital systems extend managerial oversight into new areas of workers' lives, intensify work, fragment tasks, obscure decision-making and deepen information asymmetries between employers and workers.

Digitalisation is also frequently used to bypass established industrial-relations practices. New technologies are introduced as matters of managerial prerogative; data are collected without transparency; and algorithmic decisions are presented as objective or unchallengeable.

This report starts from a different premise. Digitalisation does not suspend labour law, weaken fundamental rights

or displace collective bargaining. On the contrary, it makes union organisation, legal knowledge and collective action more necessary than ever. Existing labour law, data protection law, equality law and occupational safety and health frameworks continue to apply in digitalised workplaces, even if they must now be asserted and enforced under new conditions.

For unions, legal clarity is therefore not an abstract concern. It is a source of bargaining power. Knowing which rights already exist – and where they fall short – enables unions to challenge unilateral technological change, demand information and consultation, and negotiate binding protections that keep workers in control of how technology reshapes their jobs.

How to use this country report

This report is written for Indian workers, shop stewards, and trade unions operating in a context of extensive workplace surveillance, rapid digitalisation, and fragmented labour protection. Technologies such as CCTV, biometric attendance, GPS tracking, and AI-based management are widespread, often introduced without transparency or meaningful consent.

The report helps unions navigate India's complex legal landscape, including constitutional rights, labour codes, and evolving data-protection rules. It supports workers in asserting basic safeguards where enforcement is weak and employment relationships are increasingly mediated by digital systems.

The report includes a checklist of key questions based on legal rights that workers and unions can use *before* a new technology is introduced and periodically while it is being used. These questions are intended to structure negotiations, demand information, and prevent technologies from being imposed unilaterally or expanded without consent.

The purpose of the report is practical and strategic: it aims to support workers and unions in understanding what digitalisation means for their rights, to strengthen their position in discussions with management, and to help turn abstract legal protections into concrete, enforceable workplace standards.

No legal ecosystem fully addresses the risks to workers' rights, dignity and decent work. To bridge the gaps, the report also includes a list of potential collective bargaining topics and issues for inspiration in the negotiations with management.

Digital technologies are often introduced by management as technical upgrades, efficiency tools, or unavoidable innovations. In practice, however, they frequently reshape working conditions, intensify monitoring, redistribute power, and create new risks for workers' dignity, autonomy, health, and job security. Digitalisation is not just a technical matter, though. It is a labour issue and therefore a legitimate subject for negotiation, consultation, and collective bargaining.

What this report can do for you

This report is designed to help you:

- **Identify digital technologies** being used or proposed in your workplace, even when they are presented in vague or technical language;
- **Understand your existing rights** under labour law, data-protection rules, occupational safety and health frameworks, anti-discrimination law, and collective agreements;
- **Hold management accountable** to its legal obligations when introducing, using, or expanding digital systems;
- **Prepare for negotiations** by showing how other unions and workers have addressed similar challenges;
- **Bridge gaps in the law** through collective bargaining where legal protections are weak, unclear, or poorly enforced.

Rather than assuming that digitalisation is inevitable or uncontested, the report treats it as a process that can—and must—be shaped through collective action.

How to use this report in practice

Each section of this report serves a specific purpose and can be used independently, depending on your immediate needs.

Section 2: Examples of digital technologies used in workplaces

This section provides examples of digital technologies used in India. Maybe your workplace uses a similar technology, although it might be called something different? If you are in doubt about what digital technologies are used, do a virtual walk-through of a typical working day.

From the moment you enter the workplace – how do you get in? Do you use an electronic keycard? Or does a technology register your fingerprint or face? Do you then need to log on to a computer technology, use a handheld device, a mobile phone, a GPS tracker, or anything else? All of these technologies are digital, and all of them create data.

If your walk-through reveals the use of digital technologies at work, this report will be highly useful for you.

Section 3: What are your rights – and what are management's obligations?

This section begins with a graphical depiction of the legal and collective frameworks that already apply to digitalised workplaces. You can use this section to quickly identify which laws, regulations, or agreements are relevant to your situation. Find the links to the laws and agreements in the Annex.

It then moves on to describe the legal and collective frameworks that already apply to digitalised workplaces. It explains what employers are required to do—such as consult workers, assess risks, limit surveillance, or ensure fairness—and how unions can invoke these obligations in discussions, negotiations, or disputes.

Section 4: The checklists of questions you have a right to ask!

Cut out this section and carry it with you when you prepare for discussions with management around the implementation and use of digital technologies in your workplace.

The questions help ensure that your rights are respected and that employers meet their obligations.

Section 5: Filling the Gaps – Bargaining Topic Suggestions

Even when management follows the law, the law is often not enough to address how digital systems affect every day working conditions. Many of the issues raised by AI, monitoring tools, performance dashboards, and data-driven management are only partially regulated or not regulated at all by existing legislation. This is where collective bargaining becomes important. This section provides examples of bargaining themes that unions may consider when seeking to address the gaps that current law leaves open.

For further inspiration on concrete contract language unions have successfully negotiated, see Public Service International's open database that includes almost 600 clauses related to the digitalisation of work. Find it here: <https://publicservices.international/digital-bargaining-hub>

When can you use the report?

You can use this report at different moments:

- **Before a technology is introduced**, to demand information, consultation, and justification;
- **After a system is in place**, to assess whether management is complying with its obligations;
- **During collective bargaining**, to propose concrete clauses that regulate digitalisation;
- **For education and organising**, to build shared understanding and collective confidence among workers.

Digital technologies do not manage themselves. Employers make choices about how they are deployed, and those choices can be questioned, negotiated, and reshaped. This report is intended to support you in doing exactly that.

2.

Examples of Digital Technologies Used at Workplaces in India

Workplaces in India have seen the permeation of digital technologies for monitoring employee activities and workforces. Some of the technologies that are prevalent at Indian workplaces are listed below:

1. Closed Circuit Television (CCTV)

CCTV is a surveillance system that allows monitoring of multiple locations, enhancing security by reducing personnel costs and enabling overlapping camera coverage to prevent intrusions¹. In India, CCTV monitoring is often used to ostensibly comply with women safety laws, security regulations, prevent or identify criminal activities and comply with labour laws. For instance, the Delhi Government recently permitted women to take up night shifts in shops and commercial establishments with the caveat that appropriate accommodations such as CCTV surveillance, transport etc. are provided by employers². Similar policies can be found in West Bengal³, Meghalaya⁴ etc. In Karnataka all public and private establishments are required to undertake CCTV surveillance in areas with a likelihood of public gathering of hundred people or more at a time, or of five hundred per day, including areas that fall within the ambit of a workplace⁵.

2. Biometric attendance systems

In public employment, the Biometric Attendance System ("BAS") is a part of the "Digital India" program of the Government of India. BAS has been implemented in numerous Union and State Government Offices. The system enables employees to record attendance by simply presenting their biometrics (fingerprint/Iris) in the installed biometric devices, that are authenticated online from the biometric data (Aadhaar) stored in Unique Identification Authority of India (UIDAI)⁶. Such systems are being actively used to track attendance of employees of Municipal Corporations⁷, sanitation workers⁸ staff at universities⁹, Transport Corporations¹⁰, and hospitals¹¹. Reports suggest that close to 7,500 Union and state government organisations, where about 900,000 central and 1.7 million state employees work, may have been using over 80,000 such suspect biometric attendance systems¹². The BAS was largely developed by the National Informatics Centre, and consists of a number of components manufactured by various companies such as Mantra Softtech India Pvt Ltd, Matrix Comsec etc. Reports suggest that some of the companies procuring components for the BAS may be using microchips and hardware manufactured by Chinese companies, creating cyber security risks¹³.

1 Philip P. Purpura, "External Threats and Countermeasures", Editor(s): Philip P. Purpura, Security and Loss Prevention (Fifth Edition), Butterworth-Heinemann, 2008, Pages 175-210, ISBN 9780123725257, <https://doi.org/10.1016/B978-0-08-055400-6.50014-5>

2 Press Trust of India, "Female security, CCTV surveillance: How the Delhi Government is making night shifts safer for women", (The Hindustan Times, 29 July, 2025), <https://www.hindustantimes.com/india-news/female-security-cctv-surveillance-how-delhi-govt-is-making-night-shifts-safer-for-women-101753811871738.html>

3 Anirban Sinha Roy, "West Bengal to implement new workplace safety guidelines for women" (India Today, 1 August, 2025) <https://www.indiatoday.in/india/story/west-bengal-to-implement-new-workplace-safety-guidelines-for-women-2764496-2025-08-01>

4 India TodayNE, "Meghalaya clears policy change allowing women to work night shifts with safety measures" (India Today, 8 August, 2025) <https://www.indiatodayne.in/meghalaya/story/meghalaya-clears-policy-change-allowing-women-to-work-night-shifts-with-safety-measures-1258043-2025-08-08>

5 Section 3, The Karnataka Public Safety (Measures) Enforcement Act, 2017, https://www.indiacode.nic.in/bitstream/123456789/8186/1/44_of_2017%28e%29.pdf

6 Government of India, "Biometric Attendance System" (2018), <https://nextcloud.fes.de/nc/s/DDN2YgGYMwr8zps>

7 Express New Service, Chandigarh: Aadhaar-enabled biometric attendance system for MC employees must from November 1 (Indian Express, 27 October, 2025), <https://indianexpress.com/article/cities/chandigarh/chandigarh-aadhaar-enabled-biometric-attendance-system-for-mc-employees-must-from-november-1-10328714/>

8 "City body's biometric attendance to monitor sanitation workers' work" (10 May, 2025) <https://timesofindia.indiatimes.com/city/nagpur/civic-bodys-biometric-attendance-to-monitor-sanitation-workers-work/articleshow/121041116.cms>

9 MF Ahmed, "NPU to use Aadhaar enabled biometric attendance system to pay staff salary" (10 October, 2025, Times of India) <https://timesofindia.indiatimes.com/city/ranchi/npu-to-use-aadhaar-enabled-biometric-attendance-system-to-pay-staff-salary/articleshow/124461437.cms>

10 N Dhamotharan, "TNSTC to enforce biometric attendance system across Tamil Nadu from June 21" (22 June, 2025, New Indian Express) <https://www.newindianexpress.com/thesundaystandard/2025/Jun/22/tnstc-to-enforce-biometric-attendance-system-across-tamil-nadu-from-june-21>

11 Aditya Saha, "Biometric attendance to be mandatory for all healthcare staff in Maharashtra" (7 March 2025, Medical Dialogues) <https://medicaldialogues.in/news/health/doctors/biometric-attendance-to-be-mandatory-for-all-healthcare-staff-in-maharashtra-144502>

12 Pradip R Sagar, "Big data breach threat from Chinese chips in govt biometric attendance" (20th Jan, 2024) <https://www.indiatoday.in/india-today-insight/story/big-data-breach-threat-from-chinese-chips-in-govt-biometric-attendance-2491261-2024-01-20>

13 Ibid.

3. Facial Recognition Technology (FRT)

In the public sector various Municipal Corporations¹⁴ including Hyderabad¹⁵, Chandigarh¹⁶, Madurai, Panchkula etc., are implementing FRT or Facial Authentication Technology to check attendance of employees. This system is said to allow employees to move naturally through designated entry and exit points where FRT cameras are placed, to automatically record attendance without employees having to pose for attendance. The Facial Authentication Technology used by Chandigarh Municipal Corporation has been administered by the National Informatics Centre (NIC)¹⁷.

Some of the major companies engaged in developing and providing facial recognition and/or authentication technology for employee monitoring in India include Indian companies like Matrix Comsec, Mantra Softtech, Truein, and Darwinbox.

4. Location, Global Positioning System (GPS) and behaviour tracking

Municipal corporations around India are mandating that sanitation workers wear GPS-enabled efficiency trackers¹⁸. For instance, the Vadodara Municipal Corporation (VMC) has developed an AI-based geo-fencing attendance system and plans to implement it for all its 4,400 employees. This system automatically registers attendance and work hours are calculated based on the time spent at the workplace¹⁹. Some GPS enabled trackers include smartwatches distributed by municipal corporations. These smartwatches have a microphone and a camera so a supervisor can hear and watch the worker. A SIM-card embedded in the tracker allows the supervisor to call the worker at any time. Similar employee surveillance systems are being used in Mysore, Lucknow, Indore, Thane, Navi Mumbai, Nagpur, and Chandigarh²⁰.

- Some of the municipal corporations have sourced these smart watches from Imtac India Private Ltd.²¹ an Indian subsidiary of IMTAC headquartered in Oman.
- Location tracking is also prevalent in all forms of platform-based gig work where the location of the delivery personnel or transport service provider is tracked by the application in real-time format and shared with the user of the platform who is availing the service from the platform worker. In India, Swiggy, Zomato, Uber, OLA, Porter are some platforms that track the location of workers.

5. AI-based monitoring system

AI-based worker tracking system is becoming prominent, especially in the delivery sector. For instance, Amazon is known to have been using a tracking software known as Associate Development and Performance Tracker (ADAPT)²² ADAPT tracks warehouse workers' productivity and determines how quickly the workers can locate, scan and box packages. Workers who do not meet the required productivity rates receive automatically generated warnings, which may lead to termination in some cases²³.

AI-based worker monitoring systems are slowly gaining traction in Indian factories and in the IT sector. For instance, a new product called Optifye.ai uses computer vision technology to track workers on assembly lines and provides factory managers with productivity data²⁴. Mahindra & Mahindra had piloted a programme that uses AI to detect employees' moods. The AI tool called a 'mood-o-meter', engages with employees throughout the day, asking questions to gauge their mood²⁵. Further, employers use AI driven tools for recruitment through virtual interviews and behaviour analysis.

14 "GHMC to deploy AI-based facial recognition to mark staff attendance" (28 October, 2025, The Times of India) <https://timesofindia.indiatimes.com/city/hyderabad/ghmc-to-deploy-ai-facial-recognition-to-mark-staff-attendance/articleshow/124857026.cms>

15 "Greater Hyderabad Municipal Corporation starts facial recognition attendance" (21 September, 2024), <https://www.newindianexpress.com/cities/hyderabad/2024/Sep/21/greater-hyderabad-municipal-corporation-starts-facial-recognition-attendance>

16 BW Online Bureau, "Chandigarh MC Makes Facial Recognition Attendance Mandatory From November" (29 October, 2025, BW People) <https://www.bwpeople.in/article/chandigarh-mc-makes-facial-recognition-attendance-mandatory-from-november-577410>

17 "Aadhaar based biometric attendance must for UT MC staff" (October 26, 2025) <https://timesofindia.indiatimes.com/city/chandigarh/aadhaar-based-biometric-attendance-must-for-ut-mc-staff/articleshow/124816603.cms>

18 Rachna Khaira, "Surveillance Slavery: Swachh Bharat Tags Sanitation Workers To Live-Track Their Every Move" (Feb 18, 2020, Huffpost) https://www.huffpost.com/archive/in/entry/swachh-bharat-tags-sanitation-workers-to-live-track-their-every-move_in_5e4c98a9c5b6b0f6b6ff11f9b

19 "VMC to roll out AI-based attendance system for staff" (15 October, 2025, The Times of India) <https://timesofindia.indiatimes.com/city/vadodara/vmc-to-roll-out-ai-based-attendance-system-for-staff/articleshow/124586746.cms>

20 Rachna Khaira, "Surveillance Slavery: Swachh Bharat Tags Sanitation Workers To Live-Track Their Every Move" (Feb 18, 2020, Huffpost) https://www.huffpost.com/archive/in/entry/swachh-bharat-tags-sanitation-workers-to-live-track-their-every-move_in_5e4c98a9c5b6b0f6b6ff11f9b

21 Misuse of GPS watches meant to track Chandigarh MC employees can't be overlooked: Audit report (11 June, 2022) <https://www.tribuneindia.com/news/chandigarh/misuse-of-gps-watches-meant-to-track-chandigarh-mc-employees-cant-be-overlooked-audit-report-402891/>

22 Somesh Jha, "Amazon faces Indian court scrutiny for labour conditions at warehouse" (30th November, 2024, AlJazeera) <https://www.aljazeera.com/news/2024/11/30/amazon-faces-indian-court-scrutiny-for-labour-conditions-at-warehouse>

23 Rachel Goldenberg, "Perils of Amazon robots that hire, fire" (LexisNexis Canada) <https://www.lexisnexis.ca/en-ca/ihc/2019-06/perils-of-amazon-robots-that-hire-fire.page>

24 Sanya Jain, "Why an AI startup by Indian founders has sparked global outrage after Y Combinator demo" (27 February, 2025) https://www.hindustantimes.com/trending/dystopian-ai-startup-by-indian-founders-sparks-global-outrage-promoting-slavery-101740540904553.html#google_vignette

25 Anjali Venugopalan, "Mahindra & Mahindra's AI bot to gauge staff mood" (23 July, 2019, The Economic Times) <https://economictimes.indiatimes.com/jobs/mahindra-mahindras-ai-bot-to-gauge-staff-mood/articleshow/70338650.cms?from=mdr>

3.

What Are Your Rights – And What Are Management’s Obligations?

Below, we set out the key rights you already have when management decides to introduce or use digital technology at work. We do this law by law, pointing you directly to the specific provisions you need to know. Alongside your rights, we also highlight management’s legal obligations to you, including duties to consult, ensure system transparency, conduct risk assessments, and more.

Then, in the next section, we bring this together into two practical sets of questions you can use to hold management to account. The first set covers questions to ask **before** a new digital technology is introduced. The second set covers your **ongoing rights** once the technology is in use. Every question is grounded in existing laws and/or collective agreements. Where management is reluctant to engage or provide answers, we reference the exact legal provisions you can rely on.



→ Union Laws

- a. Information Technology Act, 2000 & the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011
- b. Digital Data Protection Act, 2023
- c. Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013
- d. Rights of Persons with Disabilities Act, 2016
- e. Labour Codes: The Code on Wages, 2019, The Industrial Relations Code, 2020, The Code on Social Security, 2020, and the Occupational Safety, Health and Working Conditions Code, 2020

→ State Laws

- f. Shops and Establishments Laws
- g. Laws Governing platform-based gig work in the respective states: Karnataka, Jharkhand, Bihar

→ Constitution of India

- a. Article 21: Right to Life and Personal Liberty

Information Technology Act, 2000 (“IT Act”)²⁶ & the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (“SPDI Rules”)²⁷

At the time of this report, the IT Act provides for a data protection regime that also accounts for the personal data of employees. The IT Act protects ‘sensitive personal data or information’ (“SPDI”) which is defined under the SPDI Rules. It applies to organisations established in India, and organisations located outside of India, that use a computer, computer system, or computer network to process personal information and SPDI in India. Sec-

tion 43A of the IT Act provides for compensation to be paid by a body corporate where they have failed to protect SPDI and empowers the Union Government to notify ‘reasonable security practices and procedures’ to be complied with by body corporates. Hence, the Union Government has notified the SPDI Rules under the IT Act, outlining the reasonable practices and procedures to be complied with, to protect SPDI.

²⁶ https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

²⁷ [https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20\(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information\)%20Rules,%202011.&searchradio=rules](https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules)



→ **Rule 4**

The body corporate must provide policy for privacy and disclosure of information.

→ **Rule 5**

The body corporate is required to take consent and provide notice to the Data Principal before collecting sensitive personal data. The body corporate must not retain the personal data for longer than required for the purpose of collection or permitted under law, and such data must be used only for the purpose for which it was collected. Data principals must also be permitted to correct the SPDI that they have provided and to withdraw consent. The SPDI must be kept secure. The body corporate must also appoint a Grievance Redressal Officer to redress concerns of data principals under the SPDI rules, within 1 month of the date of receipt of the grievance.

→ **Rule 6**

Disclosure of information by the body corporate to any third parties will require prior consent of the data principal unless disclosure is otherwise required under law.

→ **Rule 7**

The body corporate must ensure the same level of data protection as maintained by itself prior to transferring information to any third parties. Such transfer of information is permitted only under a lawful contract.

→ **Rule 8**

The body corporate is required to maintain reasonable security practices and procedures

The SPDI Rules are applicable to 'body corporates' which are private entities and to select public entities where such entities are registered as a company or firm engaged in commercial or professional activities. The SPDI Rules will continue to remain in force until May 13, 2027, in the context of notice and consent requirements, security safeguards, and rights of data principals. These rules, with respect to the aforementioned issues, will be replaced by the DPDP Act, 2023 and the Digital Personal Data Protections Rules, 2025 ("the DPDP Rules, 2025") from May 14, 2027, onwards. 'Sensitive personal data' under the SPDI Rules includes the following information:

- passwords;
- financial information such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- biometric information;
- any detail relating to the above clauses as provided to body corporate for providing service; and
- any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

The compliances for an employer collecting SPDI under the IT Act and the SPDI Rules are specified below:

- a. Your employer must implement security practices and procedures designed to protect SPDI from unauthorised access, damage, use, modification, disclosure or impairment. (Rule 8)
- b. Your employer may collect SPDI only where collection of information is considered necessary for a lawful purpose in connection with the function or activity of the company of the employer (Rule 5 (2)). Such SPDI can be used only for the purpose for which it was collected by the employer and not for any other use case (Rule 5(5)). For instance, an employer cannot ask information about an employee's sexual orientation²⁸ as it has no nexus with the activity of the company.
- c. Your employer must not retain the SPDI for longer than necessary for the purpose for which it was collected (Rule 5(4)).
- d. Your employer must obtain specific written consent from you before collecting your SPDI. (Rule 5(1)) You must be informed as to why such SPDI is being collected, what SPDI is being collected, who will such SPDI be transferred to and the name and address of the entity collecting and storing the SPDI (Rule 5(3)).
- e. Your employer must have a privacy policy which is made available to you, and it should be available on the website of your employer (Rule 4). The privacy policy of your employer must be clear and easily ac-

²⁸ Navtej Singh Johar v. Union of India, AIR 2018 SC 4321.

cessible. It must specify the type of personal data being collected, purpose of collection and usage, disclosure to third parties (if any) and the security practices undertaken by the employer (Rule 4).

- f. Your employer must allow you to access your information to review, amend and correct it (Rule 5(6)).
- g. Your employer must provide you with an option to not provide the data or information sought to be collected. You may also have an option to withdraw consent given earlier to your employer (Rule 5(7)).
- h. Your employer must designate a 'Grievance Redressal Officer' ("GRO") to address your information concerns. The GRO must redress your grievance within one month of receipt of the grievance (Rule 5(9)).
- i. Your employer may transfer information to third parties only after ensuring that such third party maintains the same level of data protection as itself, and as required under the SPDI rules. Such transfer is per-

mitted only through a lawful contract between your employer and a third party or through consent from you for such transfer (Rule 7).

- j. Your employer must implement reasonable security practices and procedures to protect your SPDI. The SPDI rules require compliance with the International Standard IS/ISO/ IEC 27001 on 'Information Technology – Security Techniques – Information Security Management Systems – Requirements' and any other applicable standards as per prevailing laws or sector specific associations. Your employer must also undertake an audit of your security practices from time to time, by appointing an independent auditor. (Rule 8)
- k. Where an employer is negligent in implementing and maintaining reasonable security practices and procedures resulting in wrongful loss or wrongful gain to any person, such employer is required to compensate the employee for wrongful loss that you may accrue due to such non-compliance (Section 43A of IT Act).

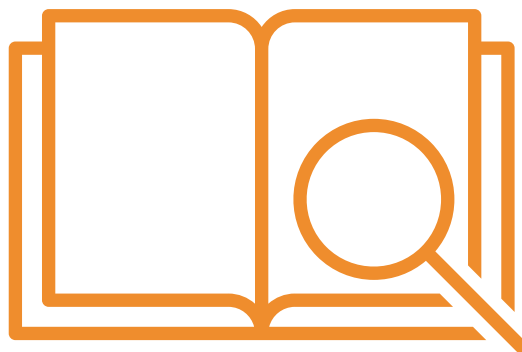
Digital Data Protection Act, 2023 ("DPDP Act")²⁹

The DPDP Act was enacted by the Indian Parliament in August 2023. The DPDP Act, 2023 provides for the processing of digital personal data in a manner that recognises the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. The DPDP Act, 2023 regulates a class of entities known as 'data fiduciaries', which process personal data of individuals. 'Data fiduciaries' means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. As per the DPDP Rules, 2025 which have been notified under the DPDP Act, 2023, the provisions on consent, notice requirements, rights of data principals, and security procedures come into force from May 14, 2027, until then the IT Act, 2000 and the SPDI Rules, 2011 will govern the aforementioned issues.

The DPDP Act applies to government and private employers collecting or processing personal data. However, processing of employment data for certain purposes has been classified as a 'legitimate use' under Section 7(i) the DPDP Act. Where an activity is classified as a 'legitimate use', consent is not required for processing personal data for such purposes. This means that employers may process personal data of employees for *'the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by the employee'* without the consent of the employee.

Considering that the DPDP Act has been notified only on 13th November 2025, the interpretation of the provisions of the Act by the Courts and industry players is undetermined as on date of this report. However, Unions must push towards a very narrow interpretation of Section 7(i) of the DPDP Act and argue for 'employee performance' not to fall within the ambit of 'legitimate uses'. Unions can argue that any surveillance which assesses the efficiency or work of the employee will not be a 'legitimate use' under the DPDP Act and requires consent of the employee or worker.

For instance, while a cab aggregator may collect a gig worker's location data since it relates to the purpose of employment, collecting real-time personal health data of the gig worker in the name of efficiency without consent would not be legitimate use.



²⁹ <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>



→ Section 4

A person may process the personal data of a data principal only in accordance with the provisions of this Act and for a lawful purpose, — (a) for which the data principal has given her consent; or (b) for certain legitimate uses.

→ Section 5

Every request for consent made to a data principal by a data fiduciary shall be accompanied or preceded by a notice given by the data fiduciary to the data principal, informing her,— (i) the personal data and the purpose for which the same is proposed to be processed; (ii) the manner in which she may exercise her rights under the Act; and (iii) the manner in which the data principal may make a complaint to the Board

→ Section 6

The consent given by a data principal (for processing her personal data) to the data fiduciary must be free, specific, informed, unconditional and unambiguous with a clear affirmative action. The consent must be specific to the personal data which is necessary to fulfil the lawful purpose for which it is collected. Requests for consent must be in clear and plain language, in English or any language of the Eighth Schedule at the option of the data principal. Consent can be withdrawn by the data principal at any time.

→ Section 7

This provision provides for certain legitimate uses of personal data for which consent is not necessary for undertaking processing activities. These legitimate uses include employment or those purposes related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a data principal who is an employee.

→ Section 8

This provision provides for the general obligations of a data fiduciary. This includes obligations to ensure completeness of information where such information will be processed to make a decision that affects the data principal or is going to be shared with a third party. It requires data fiduciaries to protect the personal data in their control and processing data by other entities on their behalf. It also requires intimation to data principles and the data protection board for any personal data breach. The provision also requires erasure of personal data on withdrawal of consent by the data principal or when the purpose of collection is no longer being served, unless retention is required under a law.

→ Section 10

This provision is applicable to Significant Data Fiduciaries who are notified based on volume and sensitivity of personal data being processed, risks to rights of data principals, among other criteria. This provision requires Significant Data Fiduciaries to appoint Data Protection Officers, undertake audits and data protection impact assessments in a periodic manner.

→ Section 11

Right to access information about personal data

→ Section 12

Right to correction and erasure of personal data

→ Section 13

Right of grievance redressal

→ Section 14

Right to nominate an individual to exercise rights on behalf of the data principal in case of death or incapacity

→ Section 33 (I) and the Schedule

Provides for the penalties for violations of the Act

Where the employee is able to establish that the purpose for which the employer is processing their personal data falls outside the scope of 'legitimate use' under Section 7(i) the DPDP Act, and that therefore consent is necessary for such processing activities, following are the key compliances for employers, under the DPDP Act-

- a. Your employer must take your free, explicit, informed, unconditional and unambiguous consent for processing your personal data. A request for such consent must be accompanied by a notice containing what personal data is going to be processed, for what purpose such data will be processed, the manner in which

the employer may exercise rights under the DPDP Act, and the manner in which you may make a complaint to the Data Protection Board, if the DPDP Act is violated. (Section 5 (1))

- b. You may manage, review or withdraw consent to prevent your personal data from being processed at any time and your employer must provide you with an easily accessible mechanism to withdraw such consent. Once you withdraw consent, your employer must cease processing your personal data within a reasonable period of time unless it is required to be retained or processed under any law (Section 6(4) and Section 6(6)).

- c. The notice provided to you for consent to process your personal data must be in a clear and plain language. You must be provided an option to access such requests in English or any language specified in the Eighth Schedule to the Constitution (Section 6(3)).
 - d. If your employer is classified as a significant data fiduciary, they are required to provide you with contact details of a Data Protection Officer, or of any other person authorised to respond to communication/s from you for exercising your rights under the DPDP Act (Section 8(9)).
 - e. Your employer may collect your personal data only where collection of such data is for a lawful purpose. Your personal data can be used only for the purpose for which it was collected by your employer (Section 4).
 - f. Your employer is required to erase your personal data as soon as it is reasonable to assume that the specified purpose for which it was collected is no longer being served. The employer is also required to ensure that anyone processing your personal data on their behalf also erases your personal data in the aforementioned circumstance. (Section 8(7))
 - g. Where the personal data processed by your employer is likely to be used to make a decision that affects you; or is going to be disclosed to a third party, your employer is responsible for the completeness, accuracy and consistency of your personal data. (Section 8 (3)).
 - h. Your employer is required to protect the personal data, which is under their control, and ensure that anyone processing it on their behalf also adopts reasonable security safeguards to prevent data breaches (Section 8(5))
 - i. If a personal data breach occurs, your employer is required to intimate you and the Data Protection Board regarding such breach (Section 8(6))
 - j. If your employer is classified as a significant data fiduciary, your employer is required to undertake a data audit by an independent data auditor and a data protection impact assessment. The data protection impact assessment must comprise a description of the rights of Data Principals, the purpose of processing of their personal data and assessment and management of the risk to the rights of the Data Principals (Section 10 (2)(b) and Section 10(2)(c)).
- As an employee whose personal data is being processed by your employer, where you are able to establish that the purpose for which the employer is processing your personal data falls outside the scope of 'legitimate use' under Section 7(i) the DPDP Act, and that therefore consent is necessary for such processing activities, you have the following data rights against your employer:
- i. Right to access information about your personal data (Section 11): You can request a summary of your personal data being processed, the purposes, and the identities of Data Fiduciaries holding it.
 - ii. Rights to correction and erasure of your personal data (Section 12): You can ask for inaccurate or incomplete data to be corrected, updated, or completed, and request deletion when it's no longer needed.
 - iii. Right to have your grievances with respect to compliance with the DPDP Act redressed (Section 13): You have the right to lodge complaints about data processing with the Data Fiduciary or Consent Manager or escalate to the Data Protection Board if unresolved.
 - iv. Right to nominate someone to exercise rights over your personal data on your behalf in case of your death or incapacity (Section 14).

Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 ("the POSH Act")³¹

The POSH Act was enacted by the Union Government to protect women from sexual harassment at the workplace. The POSH Act also applies to 'workplaces' which are defined to include both government and private sector organisations. Digital workplaces, which include virtual spaces like messaging platforms, emails, and on-

line meetings, are also included within the definition of 'workplace' because the definition of a "workplace" is broad and extends beyond physical locations. Digital interactions on platforms like WhatsApp and Facebook are considered part of the "workplace" under the POSH Act³². Hence, if you are a female employee facing sexu-

³⁰ As this Act has just come into implementation on Nov 14, 2025- the interpretation of some of these provisions are unclear. A preliminary analysis, which the Unions must also push for, is that the right to grievance redressal and right to nomination are available to workers irrespective of whether consent was the basis of for collection of personal data. There is nothing explicitly specified in Section 13 (Right to grievance redressal) and Section 14 (Right to nomination) preventing workers from availing these rights against employers.

³¹ https://doe.gov.in/files/inline-documents/DoE_Prevention_sexual_harassment.pdf

³² Amit Kumar vs. University of Delhi, W.P.(C) 586/2021 & CM APPL. 42639/2024.

al harassment online during the course of your employment, you may file a complaint with the Internal Complaints Committee constituted by your employer. Your employer is legally mandated to receive and inquire

into your complaint. Section 9 of the POSH Act provides for the manner in which a complaint may be made by a woman aggrieved by sexual harassment at the workplace.

Rights of Persons with Disabilities Act, 2016 (“the RPWD Act”)³³

The RPWD Act, 2016 enumerates and protects the rights of persons with disabilities in India. The law mandates employers to make reasonable accommodations for employees with disabilities. These accommodations extend to digital workplaces. Your employer is also required to notify an equal opportunity policy detailing measures

proposed to be taken by them in pursuance of compliance with the RPWD Act, 2016 (Section 21 of the RPWD Act, 2016 And Rule 8 of the RPWD rules, 2017)³⁴. Rule 15 also provides for compliances to make Information and Communication Technology accessible to persons with disabilities.

Labour Codes

India has four consolidated legislations governing labour. They are listed below:

Code on Wages, 2019 (“the Wage Code”)³⁵

The Wage Code unifies Indian law on universal minimum wages, mandates equal pay for equal work, ensuring timely payments and requires overtime pay at double the normal rate. The mandate to ensure equal pay for equal work extends to employers using AI, creating a requirement for employers to ensure that the automated decision-making systems that they use are free of bias and that people belonging to all genders receive equal pay for equal work. (Section 3).

Further, Article 14 of the Indian Constitution guarantees the Right to Equality against the State. The right to equality also includes the right to equal pay for equal work³⁶. The Supreme Court of India has held that the party who claims equal pay for equal work has to make necessary averments and prove that all things are equal and still there was a difference in pay³⁷, as the burden of establishing right and parity in employment is on the person claiming such right³⁸. Hence, while raising a claim of unequal pay, workers must produce proof to the effect that the work done by the claimant was the same as others, that there are similar responsibilities, qualifications and recruitment method, but that wages or salary are differing.

→ Section 3

Prohibition of discrimination on ground of gender: (1) There shall be no discrimination in an establishment or any unit thereof among employees on the ground of gender in matters relating to wages by the same employer, in respect of the same work or work of a similar nature done by any employee



Industrial Relations Code, 2020³⁹ (“the IR Code”)

The IR Code consolidates laws relating to Trade Unions, conditions of employment in industrial establishments or undertakings, and investigation and settlement of industrial disputes.

The IR Code also mandates for ‘standing orders’ to be issued by the employers in all industrial establishments employing three hundred or more workers, based on the model stand-

ing orders notified by the Central Government. Standing orders are the rules defining the conditions of work of employees. As per the first Schedule to the IR Code, the standing orders must cover the following aspects:

1. Classification of workers, whether permanent, temporary, apprentices, probationers, or those on fixed term employment;
2. Manner of intimating to workers periods and hours of work, holidays, pay-days and wage rates;

³³ <https://cdnbbsr.s3waas.gov.in/s36ee69d3769e832ec77c9584e0b7ba112/uploads/2025/03/202503251422104079.pdf>

³⁴ https://upload.indiacode.nic.in/showfile?actid=AC_CEN_25_54_00002_201649_1517807328299&type=rule&filename=Rules_notified_15.06.pdf

³⁵ <https://www.indiacode.nic.in/bitstream/123456789/15793/1/aA2019-29.pdf>

³⁶ State Of Madhya Pradesh and Another vs Pramod Bhartiya and Others, AIR 1993 SC 286.

³⁷ State Of Punjab & Anr vs Surjit Singh & Ors, CIVIL APPEAL NO. 1976 OF 2003.

³⁸ SAIL v. Dibyendu Bhattacharya, (2011) 11 SCC 122

³⁹ <https://www.indiacode.nic.in/bitstream/123456789/22040/1/A2020-35.pdf>

3. Shift working;
4. Attendance and late coming;
5. Conditions of, procedure in applying for, and the authority which may grant leave and holidays;
6. Requirement to enter premises by certain gates, and liability to search;
7. Closing and reporting of sections of the industrial establishment, temporary stoppages of work and the rights and liabilities of the employer and workers arising therefrom;
8. Termination of employment, and the notice thereof to be given by employer and workers;
9. Suspension or dismissal for misconduct, and acts or omissions which constitute misconduct;
10. Means of redress for workers against unfair treatment or wrongful exactions by the employer or his agents or servants;
11. Any other matter which may be specified by the appropriate Government by notification.

Section 30 of the IR Code provides for preparation of draft standing orders by employers and the procedure for certification. As per this provision the employer is required to consult

the trade union or the recognised negotiating union after preparing and sharing a draft of the standing orders with them. Prior to such standing orders being certified- the certifying officer who officially certifies the standing orders issued by the employer is also required to notify the trade union or workers' representatives (in the absence of trade unions) regarding the standing orders, seeking their comments. The trade union must also be provided an opportunity to be heard before the certifying officer, prior to the certification of the standing orders. A similar process is followed for modification of standing orders (Section 30(4)) under the same provision.

Unions and worker representatives should look towards negotiating conditions of termination of employment, the process of suspension or dismissal and means of redress for workers against unfair treatment or wrongful exactions, during the mandated consultation on standing orders undertaken by the employer under Section 30 of the IR Code, to bargain for rights against automated decision making, rights in favour of human intervention in automated processes, reasoned notice prior to dismissal, and rights against workplace surveillance.

→ Section 28

Requirement to certify standing orders for industrial establishments wherein three hundred or more workers are employed

→ Section 29

Making of model standing orders by the Central Government

→ Section 30

Preparation of draft standing orders by employer and procedure for certification: This provision requires the employer to provide a draft of the standing orders to the trade union or recognised

negotiating union and consultation with them prior to the same being shared with the certifying officer for certification. The certifying officer is also required to provide a copy to the trade union or worker representative seeking comments from them, prior to certifying the standing orders. The Union must also be provided an opportunity to be heard. A similar process is specified for the modification of existing standing orders.

→ First Schedule

Matters to be provided for in standing orders under the code



Social Security Code (“the SS Code”)⁴⁰

This code aims to extend social security such as provident fund, health insurance, maternity benefits, gratuity etc to all workers including organised workers, unorganised workers and platform workers. Section 60(5) of the

“SS Code” also provides, as part of maternity benefits, that in case the work assigned to a woman is of such a nature that she may work from home, the employer may allow her to do so, after availing of the maternity benefit for such period and on such conditions as the employer and the woman may mutually agree.

→ Section 60(5)

In case the work assigned to a woman is of such nature that she may work from home, the employer may allow her to do so after availing of the maternity benefit for such period and on such conditions as the employer and the woman may mutually agree.



⁴⁰ <https://www.labour.gov.in/static/uploads/2026/01/3d2c9ed6292b432a10df1a62973278ba.pdf>

Occupational Safety, Health and Working Conditions Code⁴¹

This code establishes uniform standards for worker safety, health, and working conditions across industries like factories, mines, and construction. Section 6(1)(a) of the code requires every employer to ensure that the workplace is free from hazards which may cause injury or occupational disease to employees. Section 6(1)(d) also mandates that employers must provide and main-

tain, as far as is reasonably practicable, a working environment that is safe and without risk to the health of the employees. Further, Section 14(1) states that every employee in an establishment shall have the right to obtain from the employer information relating to employee's health and safety at work and represent to the employer regarding inadequate provision for protection of his safety or health in connection with the work activity in the workplace, and if not satisfied, to the Inspector under the Act.



→ Section 6(1)

Every employer shall, (a) ensure that workplace is free from hazards which cause or are likely to cause injury or occupational disease to the employees, (d) provide and maintain, as far as is reasonably practicable, a working environment that is safe and without risk to the health of the employees;

→ Section 14(1)

Every employee in an establishment shall have the right to obtain from the employer information relating to employee's health and safety at work and represent to the employer regarding inadequate provision for protection of his safety or health in connection with the work activity in the workplace, and if not satisfied, to the Inspector-cum-Facilitator.

Shops and Establishments Laws

Most states in India have respective Shops and Establishment Acts which are state-level laws regulating working conditions in shops, commercial establishments, restaurants, and service sectors. While the state specific laws may vary, they largely cover working hours, wages, leaves (annual, sick, casual), holidays, safety, and child labour for sectors specified in the respective state laws. While these laws were conceptual-

ised at a time when digitalised workplaces were not envisaged, most of these state specific laws do not explicitly exclude tele-working arrangements. These laws are applicable to all 'establishments' and 'employees' irrespective of in-person presence. Hence, Unions and workers can rely on their respective Shops and Establishments Laws during their collective bargaining processes to bargain for better working hours, leaves etc.

Laws governing Platform-based gig work

Since 'labour' is a subject which is in the concurrent list of the Indian Constitution, both Union and State Governments are empowered to enact labour laws. Unless repealed or in conflict with the four labour codes, all such state legislation will continue to be in force and apply to workers. In addition, several state governments in India have either enacted separate laws to govern platform-based gig workers or are in the process of framing such laws. Compliances under state specific laws governing platform work which contain digital rights for platform workers are listed below.

a) Karnataka: The Karnataka Platform Based Gig Workers (Social Security and Welfare) Act, 2025⁴² ("the Karnataka Act") has not come into force as on the date of completion of this report. The Karnataka Plat-

form based Gig Workers (Social Security and Welfare) Rules, 2025 have been notified by the State Government on 19th November 2025, thus bringing the Karnataka Act into force. The Karnataka Act mandates transparency by aggregator platforms in respect of the automated monitoring and decision-making systems that they utilise. As a platform worker in Karnataka, you have the following rights:

→ Your aggregator must inform you, in simple language and in Kannada, English or any other language listed in the Eighth Schedule of the Constitution of India known to you, regarding the procedure to seek information in respect of the automated monitoring and decision-making parameters employed by them, which have an impact on your working conditions, including but not limit-

⁴¹ <https://www.indiacode.nic.in/bitstream/123456789/22041/1/a2020-37.pdf>

⁴² <https://prsindia.org/bills/states/the-karnataka-platform-based-gig-workers-social-security-and-welfare-bill-2025>

ed to fares, earnings and customer feedback (Section 13(1)).

- Your aggregator is required to take measures to prevent discrimination, by the automated systems utilised by them, on the basis of religion, race, caste,

gender, or place of birth or on the grounds of disability (Section 13 (2)).

- You are also entitled to a human point of contact, designated by the aggregator, for redressal of your grievances (Section 18).

→ Section 13

Transparency in respect of automated monitoring and decision-making systems

→ Section 18

Nomination of Point of Contact for Enquiries



b) Bihar and Jharkhand: The digital rights of platform workers under the platform worker laws in Bihar and Jharkhand are similar, hence this section provides combined digital labour compliances for aggregators.

The Gig and Platform Based Workers (Registration, Social Security and Welfare) Act, 2025 (“the Bihar Act”)⁴³ is not yet in force, and will come into force on such date/s as will be notified by the Bihar State Government. The Bihar Act mandates transparency by aggregator platforms in respect of the automated monitoring and decision-making systems that they utilise. The Jharkhand Platform Based Gig Workers (Registration and Welfare) Act, 2025 (“the Jharkhand Act”)⁴⁴ was enacted in August 2025 and is set to come into force within 120 days from its enactment or before, as notified by the Government of Jharkhand.

As a platform worker in Bihar and Jharkhand, you have the following rights under the above-mentioned Acts:

- Your aggregator must inform you, in simple language and in Hindi, English or any other language listed in the Eighth Schedule of the Constitution of India known to you, regarding the procedure to seek information in respect of the automated monitoring and decision-making parameters employed by them, which have an impact on your working conditions, including but not limited to fares, earnings and customer feedback. (Bihar-Section 13(1), Jharkhand-Section 16(1)).
- Your aggregator is required to take measures to prevent discrimination, by the automated systems utilised by them, on the basis of religion, race, caste, gender, or place of birth or on the grounds of disability (Bihar-Section 13(2), Jharkhand-Section 16(2)).

- Your aggregator must communicate the following information to you:

- the main parameters which, either individually or collectively, are the most important for determining the allocation of work, the distribution of work, the assessment of work carried out, and the grounds for denial of work;
- the rating system, if any, set up by the aggregator;
- categorisation of platform workers, on the basis of the quality of service rendered, log-in time, or any other criteria, where such categorisation is employed by the aggregator;
- the personal data of the respective platform workers available with the aggregator, such personal data which is processed by the aggregator, including the purposes for which such personal data is processed;
- any other information that may be notified by the State Government (Bihar-Section 13(3), Jharkhand-Section 16(3)).

- In cases of account deactivation, suspension, or significant reduction in work opportunities, your aggregator must provide you with:

- a written explanation outlining the specific reasons;
- the data or actions that led to the decision;
- an opportunity to appeal or request review of the decision within a stipulated timeframe (Bihar-Section 13(5), Jharkhand-Section 16(4)).

⁴³ As on the date of this report, this Act is awaiting the assent of the Governor as this is a necessary pre-requisite before the Bill becomes a law. Link to the Act, https://prsindia.org/files/bills_acts/acts_states/bihar/2025/Act8of2025BR.pdf

⁴⁴ As on the date of this report, this Act is awaiting the assent of the Governor as this is a necessary pre-requisite before the Bill becomes a law, <https://shramadhan.jharkhand.gov.in/ftp/WebAdmin/documents/Gig-worker-social-security.pdf>

→ You have the right to request a review of the algorithmic decisions of the platform (Bihar-Section 13(6), Jharkhand-Section 16(5)).

→ Your aggregator must establish a mechanism for timely redressal of your grievances. Such a redressal mechanism must have human oversight (Bihar-Section 13(6), Jharkhand-Section 16(5))



→ **Section 13 (Bihar) and Section 16 (Jharkhand)**

Transparency in respect of automated monitoring and decision-making systems.

Constitution of India: Article 21/Judicial Precedents⁴⁵

*Justice K.S. Puttaswamy (Retd.) v. Union of India*⁴⁶: According to the Supreme Court of India, the 'right to privacy' is a fundamental right of every individual traceable to the 'right to life and personal liberty' protected by Article 21 of the Indian Constitution. The Court recognised the importance of informational privacy as an aspect of the right to privacy. It made the following observations on the intersection of informational privacy and liberty.

→ Privacy is the constitutional core of human dignity.

→ Electronic tracks contain powerful means of information which provide knowledge of the sort of person that the user is and her interests. Individually, these information silos may seem inconsequential. In aggregation, they disclose the nature of the personality: food habits, language, health, hobbies, sexual preferences, friendships, ways of dress and political affiliation. In aggregation, information provides a picture of the being: of things

which matter and those that don't, of things to be disclosed and those best hidden.

→ The sphere of privacy stretches at one end to those intimate matters to which a reasonable expectation of privacy may attach. It expresses a right to be left alone. A broader connotation which has emerged in academic literature of a comparatively recent origin is related to the protection of one's identity. Data protection relates closely with the latter sphere. Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual.

→ Another aspect which data protection regimes seek to safeguard is the principle of non-discrimination which ensures that the collection of data should be carried out in a manner which does not discriminate on the basis of racial or ethnic origin, political or religious beliefs, genetic or health status or sexual orientation.

⁴⁵ <https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcd1b99b5d8f/uploads/2024/07/20240716890312078.pdf>

⁴⁶ (2017) 10 SCC 1

4.

The Checklists of Questions You Have a Right to Ask!

You are not expected to be a technology expert in order to protect your rights at work. What matters is knowing which questions you are entitled to ask **before** a digital system is introduced and **while** it is in use.

The following checklists translate existing legal rights into practical questions that workers and union representatives can use in discussions with management. Print these questions and keep them with you when preparing for, and

meeting with, management about digital technologies. Their purpose is to help ensure that existing laws and rights are properly respected in the introduction and use of digital systems at work.

Questions that workers in general can ask are listed first, followed by specific questions for platform workers in Karnataka, Bihar and Jharkhand respectively.

Workers (General)

Note: Some rights and protections (such as the right to access information on personal data and the right to correction and erasure of personal data) under the DPDP Act may be applicable to employees only in circumstances where they are able to establish that the purpose for which their personal data is being processed is not a legitimate use under Section 7 of the DPDP Act and that consent is required for such processing activities by the employer.

Section 7(i) provides that processing 'for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee' are legitimate grounds for processing data and

hence consent for such processing is not required. Where consent is not the basis for processing personal data, some rights such as the right to grievance redressal and the right to nominate a person to exercise rights may still be available to the data principal while other rights such as the right to access information on personal data and the right to correction and erasure of personal data are not.

Employees must first question the employer as to how and why the employer's processing of the respective employees' personal data should be exempted from consent requirements under Section 7(i) of the DPDP Act. Where the employer is unable to establish that the personal data is exempted from such consent requirements, the employees may proceed to demand all rights that are available to data fiduciaries under the DPDP Act.



Questions you should ask prior to the introduction of new technologies...

Checklist 1

Is my personal data being collected to safeguard the management or employer from any of the following, if so, how is this personal data going to serve the same: a. as prevention of corporate espionage, b. maintenance of confidentiality of trade secrets, c. intellectual property, d. classified information e. provision of any service or benefit sought by me	Section 7(i) of the DPDP Act
Are you collecting personal data using this digital system/technology? What kind of personal data are you collecting?	Section 5(2)(a)(i) of the DPDP Act
What purpose will my personal data be used for?	Rule 5 (3) (b) of the SPDI Rules and Section 5 (1)(i) of the DPDP Act
How long will you retain my personal data?	Rule 5(4) of the SPDI Rules Subsections (7)(a) and (8) of Section 8 of the DPDP Act
How do I exercise my rights under the DPDP Act?	Section 5(2)(a)(iii) of the DPDP Act
How do I make a complaint to the Data Protection Board if you violate the provisions of the DPDP Act?	Section 5(2)(a)(ii) of the DPDP Act
Can you share the consent notice in _____ (any language in the Eighth Schedule of the Indian Constitution/ English) language?	Section 5(3) of the DPDP Act
Where can I access your privacy policy?	Rule 4 of the SPDI Rules Section
Where can I access your privacy notice?	Section 5(1) of the DPDP Act
Why do you require my biometric data (or any category of data that you would not like to share with your employer)? Is this relevant to your activities?	Section 5(2) (a) and (b) of the SPDI Rules Section 6 (1) of the DPDP Act
What security safeguards have you undertaken to protect the personal data that you collect? Where can I access your information security program?	Rule 8 of the SPDI Rules Section 8(5) of the DPDP Act
What is the process for me to withdraw consent for processing some of the personal data that I have shared with you?	Rule 5(7) of the SPDI Rules Section 6(4) of the DPDP Act
Do you have an equal opportunity policy as required under the RPWD Act? What measures have you taken to make your digital technologies accessible to persons with disabilities?	Section 21 of the RPWD Act Rule 15 of RPWD rules
For industrial establishments with three hundred or more employees: 1. Have standing orders been notified by the management? 2. Has the process specified in Chapter IV of the Code on Industrial Wages been complied with by management for certifying standing orders? Will the standing orders be amended to account for the introduction of this new technology. If not, why? 3. How will the new technology affect termination of my employment, the process of suspension or dismissal and means of grievance redressal against unfair treatment or wrongful exactions?	Chapter IV and First Schedule of the Industrial Relations Code, 2020.

Questions you periodically should ask after the deployment of digital technologies...

Who has my personal data been shared with?	Rule 6 of the SPDI Rules Section 11(1)(b) of the DPDP Act
What are the security safeguards undertaken by the third party with whom my personal data has been shared?	Rule 7 and Rules 8 of the SPDI Rules Section 8(5) of the DPDP Act
Has the purpose of digital technology changed since it was initially deployed?	Rule 5 (3) (b) of the SPDI Rules Section 5 (1)(i) of the DPDP Act
Have you undertaken an audit of security practices? If so, when was the last time that you have undertaken such an audit?	Rule 8(4) of the SPDI Rules
If you are a significant data fiduciary under the DPDP Act: Have you undertaken data protection impact assessment?	Section 10 (c)(ii) of the DPDP Act
Has management designated a Grievance redressal officer or a data protection officer?	Section 5(9) of the SPDI rules Section 10 (2) of the DPDP Act
Whom do I approach in the event that I wish to withdraw consent from my data being processed or if I wish to update, amend or correct my personal data? How do I withdraw the consent that I had given for processing my personal data?	Section 5(9) of the SPDI rules read with Rule 5(7) of the SPDI Rules; Section 10 (2) of the DPDP Act read with Section 6(4) of the DPDP Act

Additional questions for platform workers (Karnataka)

Questions you should ask the aggregator...

What automated monitoring and decision-making system is used by you to make decisions about workers? How does it function? How does it affect my fares, earnings, customer feedback and allied information?	Section 13(1) of the Karnataka Gig Workers Act
Please provide the above information in _____ language (any language in the Eighth Schedule of the Indian Constitution or English)	Section 13(1) of the Karnataka Gig Workers Act
What measures have you undertaken to prevent discrimination by your automated system, on the basis of religion, race, caste, gender, or place of birth or on the grounds of disability?	Section 13(2) of the Karnataka Gig Workers Act
Who is my point of contact for enquiries regarding clarifications on your compliance with the Karnataka Gig Workers Act?	Section 18 of the Karnataka Gig Workers Act

Questions you should ask the aggregator...

Checklist 4

What automated monitoring and decision-making system is used by you to make decisions about workers? How does it function? How does it affect my fares, earnings, customer feedback and allied information?	Section 13 (1) of the Bihar Gig Workers Act; Section 16(5) of the Jharkhand Gig Workers Act
Please provide the above information in _____ language (any language in the Eighth Schedule of the Indian Constitution or English)	Section 13 (1) of the Bihar Gig Workers Act; Section 16(5) of the Jharkhand Gig Workers Act
What measures have you undertaken to prevent discrimination by your automated system, on the basis of religion, race, caste, gender, or place of birth or on the grounds of disability?	Section 13 (2) of the Bihar Gig Workers Act; Section 16(5) of the Jharkhand Gig Workers Act
What are the main parameters which, either individually or collectively, are the most important for determining the allocation of work, the distribution of work, the assessment of work carried out, and the grounds for denial of work?	Section 13 (3) of the Bihar Gig Workers Act; Section 16(5) of the Jharkhand Gig Workers Act
What is the rating system adopted by you?	Section 13 (3) of the Bihar Gig Workers Act; Section 16(5) of the Jharkhand Gig Workers Act
Is there any internal categorisation of workers on the basis of the quality of service rendered, log-in time, or any other criteria? If yes, please explain such categorisation and how that affects me as an employee.	Section 13 (3) of the Bihar Gig Workers Act; Section 16(5) of the Jharkhand Gig Workers Act
In the event that your account on the platform is deactivated or you are not being allotted work by the platform: a. Why is my account being deactivated or why is work not being allotted to me? b. What data or actions have led to the decision to deactivate my account or prevent me from receiving work on the platform?	Section 13 (5) of the Bihar Gig Workers Act Section 16(5) of the Jharkhand Gig Workers Act
How do I redress my grievances regarding the platform or its decisions?	Section 13 (6) of the Bihar Gig Workers Act Section 16(5) of the Jharkhand Gig Workers Act
What is the process to request a review of the algorithmic decisions undertaken by your platform which is now affecting my livelihood?	Section 13 (6) of the Bihar Gig Workers Act Section 16(5) of the Jharkhand Gig Workers Act

5.

Filling the Gaps – Bargaining Topic Suggestions

Existing law does not fully address many of the practical problems created by AI, monitoring technologies, and data-driven management at work. Collective bargaining is therefore an important way for unions to address these gaps. This section provides examples of negotiating themes that unions may draw on when developing their own demands to regulate how digital systems affect working conditions.

1. If the employer has introduced geo-fencing by mandating employees to download certain applications on their mobile devices which enables them to track your movement and record attendance, clock in and out of work, register sick days, holidays and change shifts, workers can bargain for the following:

- Restrictions on collection: That the app cannot collect location data outside of working hours or during break hours. Workers must have the right of access to the logged data.
- The employer must provide an alternative for employees or workers (other than platform workers) who do not have a smartphone to install such an application
- Natural justice principles: If such geo-fencing data is used to decide salary and pay of employees and workers, then the employer must provide a redressal mechanism when such a system is inaccurate, or failures occur in the system. Natural justice principles must be followed by an employer while taking any punitive action against workers or employees.
- Rights of Access: That the worker and their representative must receive a copy of the data, if the employer is using it in disciplinary cases. For example, if the employer claims that data from the app shows that the worker is taking longer breaks than permitted, or is stopping work early, the worker and his or her representative must have access to this raw data.

2. If the employer has introduced Facial Recognition Technology (FRT):

- Where female employees are uncomfortable with recording images via FRT, alternative mechanisms must be provided by the employer to record attendance.⁴⁷

3. If the employer has introduced CCTV surveillance:

- CCTV cannot be set up in changing rooms, locker rooms, nursing rooms and washrooms where employees and workers have a reasonable expectation of privacy.⁴⁸
- Employees must be informed prior to installation of CCTV cameras at the workplace
- Information and footage collected by CCTVs can only be used for security, safety and labour compliances under laws and should not be used to monitor the work performance of the employee.

4. If the worker is adversely affected by an automated decision, they can request human review on the grounds that natural justice principles dictate that he is entitled to a fair hearing and a reasoned decision for any action taken against him.

5. Workers may bargain for their employers to notify and certify standing orders under the IR Code, 2020. Some of the key topics that are mandated to be covered through standing orders include termination, suspension, dismissal and grievance redressal. During the consultation process for certifying standing orders, the following terms may be sought by trade unions and worker representatives from employers:

- d. Human oversight over automated decisions:** Unions must push for human oversight and reasoned orders over every automated decision that may result in a negative change in employment status of a worker. Measures must be put in place to ensure that such a human review is not merely mechanical, but is a decision taken independent of the automated decision.
- f. Access to data during disciplinary proceedings:** Unions must push for clauses that allow for workers to access the data used by the employer during disciplinary proceedings, to allow them to effectively represent their case. For example, if the employer claims that data from the app shows that the worker is taking longer.

⁴⁷ Mahesh Kumar Koli v. State of M.P., 2025 SCC OnLine MP 1773.

⁴⁸ Paramvir Singh Saini v. Baljit Singh, AIR 2021 SC 64.

- g. Union consultation prior to introduction of new technologies:** The standing orders must include a clause that requires a consultation with trade unions or recognised worker representatives, prior to introduction at the workplace. Further consultation must be sought periodically for any major changes or updates to a technology, once it is introduced.
- h. Transparency in the automated decision-making systems:** Unions may seek that employers must communicate the following information to workers:
- the main parameters which, either individually or collectively, are the most important for determining the allocation of work, the distribution of work, the assessment of work carried out, and the grounds for denial of work;
 - categorisation of workers, on the basis of the quality of service rendered, log-in time, or any other criteria, where such categorisation is used by the employer;
 - the personal data of the respective platform workers available with the aggregator, such personal data which is processed by the employer, including the purposes for which such personal data is processed;
 - Any rating system that may be utilised by the employer
- i. Restrictions on collection of data and access rights:** That the employer must not collect personal data outside of working hours or during break hours. Workers must have the right of access to the logged data.
- j. Appointment of a grievance officer:** Unions may seek the appointment of a dedicated officer to address issues faced by them due to automated decisions, collection of personal data, workplaces surveillance etc.

6.

Summary Reflections

If you remember only one thing from this report, remember this: digital systems do not remove your rights - they give you new reasons to use them!

India is at the cusp of implementing privacy protections across all sectors- be it healthcare, financial services, e-commerce, or employment. With the Digital Personal Data Protection rules being notified by the Union Government at the time of this report, the jurisprudence and shape of the data protection regime is yet to be seen. However, it is pertinent to note that the DPDP Act, 2023 is a step back in terms of its treatment of employee personal data. The exemption from consent requirements provided under Section 7(i), for processing employee personal data for the purposes of employment or those related to safeguarding the employer from loss or liability, provides broad scope for employers to misuse employee personal data without employees having sufficient forums for redress. Trade unions and worker representatives should bargain for the most strict and narrow interpretation of this exemption clause. Legislators must also consider amending the DPDP Act to provide exhaustive grounds on which employee personal data may be processed under Section 7.

Platform work remains the only sector in labour with specific laws directing transparency in the automated decision-making systems used by aggregators and mandating non-discrimination. These laws too are applicable only in some states and are yet to come into force in some of the states in which they have been enacted.

Despite the labour codes being a recent development in India, they are gravely lacking in addressing the perils of a digitalised workplace. Some principal shortcomings include the lack of mandates regarding information access and consultation mechanisms with workers prior to implementation of digital technologies and the absence of requirements for employees to appoint a human point of contact for grievance redressal in the event of loss caused to the employee due to the decision of an automated decision-making system, and a lack of provisions on risk assessment prior to introduction of digital tools at workplaces. Another glaring absence in the occupational health laws is any mention regarding the mental health of workers. There is also an urgent need for the laws regarding standing orders to be strengthened to include digitalised aspects of work, and for the prompt implementation of the standing orders across sectors.

Especially with the rise in AI tools to monitor workers, we see that technology is beginning to go beyond performance evaluation and stepping into the domain of employee behaviour analysis. Hence, there is an urgent need to regulate AI to prevent its adverse and wrongful impact on workers, and mandate transparency in the decision-making of AI tools to enable workers to understand the effects it has on them. Especially in the absence of a law governing AI in India, the scenario in India leaves little bargaining power in the hands of workers to negotiate or opt out of the use of digital technologies at their workplace.

There is also a concerning trend of governments hurriedly turning towards geo-fencing and FRT technologies through smart watches and mobile applications, to closely monitor workers on field-based work such as sanitation, community health workers, etc. without fully assessing privacy considerations in this context or providing for redressal mechanisms to those adversely affected by automated decisions by these technologies.

Employee monitoring is common in India, and even a legal requirement under some labour laws. However, the level of monitoring is inching towards surveillance, likely to affect worker well-being. While the implementation of the DPDP Act is likely to bring some relief for workers, in the absence of specific workplace regulations governing privacy, workers' involvement in the introduction of new technologies and laws on AI, workers will continue to be deprived of crucial labour rights in digitalised workplaces.

7.

Annex – Links to the Laws Covered

→ Information Technology Act, 2000

PDF here: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

→ Digital Data Protection Act, 2023

PDF here: <https://www.meity.gov.in/static/uploads/2024/06/2bf1foegfo4e6fb4f8fef35e82c42aa5.pdf>

→ Rights of Persons with Disabilities Rules, 2017

PDF here: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_25_54_00002_201649_1517807328299&type=rule&filename=Rules_notified_15.06.pdf

→ Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013

PDF here: https://doe.gov.in/files/inline-documents/DoE_Prevention_sexual_harassment.pdf

→ Code on Wages, 2019

PDF here: <https://www.indiacode.nic.in/bitstream/123456789/15793/1/aA2019-29.pdf>

→ Industrial Relations Code, 2020

PDF here: <https://www.indiacode.nic.in/bitstream/123456789/22040/1/A2020-35.pdf>

→ Occupational Safety, Health and Working Conditions Code, 2019

PDF here: <https://www.indiacode.nic.in/bitstream/123456789/22041/1/a2020-37.pdf>

→ The Code on Social Security, 2020

PDF here: <https://www.indiacode.nic.in/bitstream/123456789/16823/1/aA2020-36.pdf>

→ Karnataka Gig Workers Act, 2025

PDF here: <https://prsindia.org/bills/states/the-karnataka-platform-based-gig-workers-social-security-and-welfare-bill-2025>

→ Bihar Platform Based Gig Workers (Registration, Safety, and Welfare) Act, 2025

As on date of this report, this Act is awaiting the assent of the Governor as this is a necessary pre-requisite before the Bill becomes a law.

PDF here: https://prsindia.org/files/bills_acts/acts_states/bihar/2025/Act8of2025BR.pdf

→ Jharkhand Gig Workers Act, 2025

As on date of this report, this Act is awaiting the assent of the Governor as this is a necessary pre-requisite before the Bill becomes a law.

PDF here: <https://shramadhan.jharkhand.gov.in/ftp/WebAdmin/documents/Gig-worker-social-security.pdf>

→ Constitution of India

PDF here: <https://cdnbbsr.s3waas.gov.in/s380537a-945c7aaa788ccfcd1b99b5d8f/uploads/2024/07/20240716890312078.pdf>

8.

Glossary List

This glossary explains recurring terms and concepts used throughout the country chapters. It is intended to support workers and union representatives in quickly understanding technical, legal, and managerial language commonly used in discussions about digitalised workplaces.

A

Algorithmic management The use of software systems and algorithms to allocate tasks, evaluate performance, determine pay, schedule work, or discipline workers, often with limited transparency or human oversight.

Artificial intelligence (AI) Computer-based systems designed to perform tasks that typically require human judgment, such as decision-making, pattern recognition, prediction, or classification. In workplaces, AI is increasingly used in recruitment, performance management, surveillance, and automation.

AI systems (Artificial Intelligence systems) An AI system is a type of digital system that uses computational methods such as machine learning, statistical models, or rule-based algorithms to generate outputs including predictions, classifications, recommendations, or decisions based on input data. AI systems are used in some workplaces for tasks such as recruitment screening, performance scoring, task allocation, or pattern recognition. AI systems are digital systems that use algorithmic models to generate outputs from data.

Automated decision-making (ADM) Decisions affecting workers that are made wholly or primarily by digital systems, with minimal or no human intervention, for example in hiring, scheduling, performance scoring, or dismissal.

B

Biometric data / biometric systems Personal data based on physical or behavioural characteristics, such as fingerprints, facial images, iris scans, or voice patterns, used to identify or authenticate workers, often for attendance, access control, or monitoring.

C

Collective bargaining Negotiations between workers' organisations and employers to determine working conditions, rights, and obligations. In the context of digitalisa-

tion, collective bargaining is used to regulate technology use where law is absent, weak, or insufficient.

Consultation and worker participation Legal or collectively agreed processes requiring employers to inform and involve workers or their representatives before introducing technological, organisational, or operational changes that affect working conditions.

D

Data Any representation of information, facts, or concepts in a form capable of being processed by a computer system.

Data Fiduciary / Controller The entity (usually the employer) that decides how and why personal data is processed and bears the legal responsibility for its protection.

Data Minimisation The principle that only the data strictly necessary for a specific, stated purpose should be collected and used.

Data protection Rules and principles governing how information relating to an identifiable person is collected, stored, used, shared, and retained. In workplaces, this includes amongst others attendance data, location data, performance metrics, and biometric information.

Data Protection Impact Assessment (DPIA) A structured assessment required in many jurisdictions before introducing high-risk data-processing systems. It evaluates risks to workers' rights and freedoms.

Digital labour platforms / platform work Work mediated through digital applications or online platforms that allocate tasks, manage performance, and process payment, often using algorithmic systems. Examples include ride-hailing, delivery, and online outsourcing.

Digital technologies Digital technologies are electronic tools, devices, software, and data-processing applications that create, collect, store, transmit, or analyse digital data. In workplaces, this includes items such as computers, mobile devices, biometric scanners, cameras, GPS devices, software applications, platforms, and databases. These technologies generate and process data that can be used in organising, monitoring, or managing work. Digital technologies are the individual electronic tools and applications.

Digital systems A digital system is an arrangement of multiple digital technologies that operate together to collect data, process it according to defined rules or instructions, and produce outputs. A digital system may include hardware, software, data storage, and interfaces used by managers or workers. The system refers to the combined operation of these components rather than any single device or application. Digital systems are combinations of digital technologies working together.

Digital surveillance / worker monitoring The use of digital tools to observe, record, or analyse workers' activities, movements, communications, or performance, including CCTV, GPS tracking, keystroke logging, and screen monitoring.

E

Enforcement gaps The disconnect between formal legal rights and their real-world application, often due to weak oversight, delayed remedies, limited access to regulators, or reliance on individual complaints.

F

Function creep The gradual expansion of a technology's use beyond its original stated purpose, for example when security or attendance systems are later used for performance evaluation or discipline.

H

Human oversight The requirement that automated or AI-driven systems remain subject to meaningful human review, judgment, and accountability, particularly when decisions affect workers' rights or livelihoods.

I

Informational asymmetry A power imbalance in which employers control access to information, data, and system logic, while workers lack insight into how technologies operate or how decisions are made.

O

Occupational safety and health (OSH) Legal and organisational obligations to protect workers' physical and mental well-being at work, including risks arising from stress, work intensification, constant monitoring, or technological change.

P

Platform worker classification The legal determination of whether platform workers are treated as employees, self-employed, or a separate category, which affects access to labour rights, social protection, and collective bargaining.

Power asymmetry An imbalance of authority and control between management and workers, intensified in digitalised workplaces through surveillance, data extraction, and algorithmic control.

Purpose limitation A core data-protection principle requiring that data collected for one specific purpose (e.g. security) not be reused for incompatible purposes (e.g. discipline or productivity scoring) without justification and consultation.

R

Right to explanation / transparency The principle that workers should receive clear, accessible information about what data are collected about them, how technologies function, and how decisions affecting them are made.

Right to disconnect The right of workers to be free from work-related digital communication and monitoring outside working hours, protecting rest time and work-life boundaries.

Risk assessment An evaluation of potential harms associated with introducing new technologies, including impacts on privacy, health, equality, workload, and job security.

S

Surveillance capitalism / data extraction A model in which value is generated by collecting and analysing large amounts of behavioural data, increasingly applied within workplaces through digital management systems.

W

Worker dignity and autonomy Foundational labour principles recognising workers as rights-bearing individuals, not merely data points or inputs, requiring limits on intrusive monitoring and automated control.

About the authors

Deepa Padmar, Senior Resident Fellow

Alok Prasanna Kumar, Co-founder and Senior Project Fellow

Vidhi Centre for Legal Policy, India

Negotiating Digitalised Workplaces – Rights and Obligations

This series of country studies – encompassing to date Albania, Brasil, India, Ireland, Kenya, South Korea, and Uruguay – highlights the institutional power resources of workers to shape the digitalisation of workplaces. By knowing rights, laws and labour market agreements, workers and trade unions can henceforth better claim their rights and negotiate working conditions when digital technologies are introduced and used.

Further information on this topic can be found here:

➤ fes.de/lnk/negotigirights