THE INVISIBLE EMPLOYEE: ALGORITHMIC MANAGEMENT, DEEMED CONSENT, AND THE LIMITS OF THE DPDP ACT IN INDIA'S GIG ECONOMY

Arunima Jha, High Court of Bombay

ABSTRACT

India is home to one of the world's fastest-growing gig economies. The Niti Aayog estimates approximately 7.7 million gig workers were engaged in platform-based work in 2020-21, a figure projected to reach 23.5 million by 2029-30. These workers operate in a legal interstice: classified neither as employees entitled to labour law protections nor as independent contractors possessed of genuine entrepreneurial autonomy. Their relationship with the platforms that deploy them is mediated almost entirely through algorithmic systems that determine the work they receive, the rates they are paid, the ratings by which their livelihoods are assessed, and the terms under which they may be deactivated with no opportunity to be heard. Each of these functions involves the collection, processing, and application of personal data at scale. The Digital Personal Data Protection Act, 2023 (DPDP Act) is the primary legislative framework governing this processing. This article argues that the DPDP Act's deemed consent provisions, as currently drafted, are structurally inadequate to protect gig workers from the privacy harms of algorithmic management. The deemed consent framework was designed with a standard employment relationship in mind. It does not account for the specific vulnerabilities of platform workers, whose data processing occurs in conditions of acute informational asymmetry and without the procedural protections that employment law would otherwise supply. Drawing on Indian constitutional jurisprudence, the Supreme Court's landmark right to privacy decision, international comparative frameworks including the European Union's Platform Work Directive, and the United Kingdom Supreme Court's decision in Uber BV v. Aslam, the article argues for three specific interventions in the DPDP implementing rules: a gig worker-specific deemed consent schedule, a mandatory explainability requirement for automated deactivation decisions, and a data minimisation standard calibrated to the algorithmic management context.

Keywords: DPDP Act 2023, Gig Economy, Algorithmic Management, Deemed Consent, Gig Workers, Right to Privacy, Puttaswamy, Platform Work Directive, Data Fiduciary, Code on Social Security 2020.

INTRODUCTION

In the summer of 2022, a delivery worker in Mumbai was deactivated from a major food aggregator platform after his rating dropped below the platform's threshold. He received a notification on his phone. There was no explanation of which orders had contributed to the rating decline, no information about what customer feedback had been received, no opportunity to respond, and no internal appeals process that he could navigate without assistance. His sole source of income was gone. The platform's terms of service, which he had agreed to on a touchscreen at a registration centre, provided that deactivation was within the platform's sole discretion.[1]

This is not an isolated incident. It is the routine operation of algorithmic management in India's gig economy. Platforms exercise control over their workers through data systems that are opaque by design, consequential by operation, and legally unaccountable by the architecture of current Indian law. The worker's personal data, comprising his location history, his acceptance rate, his delivery times, his customer ratings, and in some cases his biometric identifiers, is continuously collected, processed, and applied to decisions that determine his ability to earn a living. He consented to all of this. He had no realistic alternative.

The DPDP Act, which received Presidential assent on August 11, 2023, is the most significant development in Indian data protection law since the Information Technology Act, 2000.[2] It creates a framework of data principal rights, data fiduciary obligations, and a Data Protection Board with enforcement jurisdiction. Yet for the gig worker in Mumbai, its protections are, as this article argues, largely theoretical. The deemed consent provisions of Section 7, which apply to employment-related processing without the requirement for explicit consent, were not designed with platform workers in mind. The implementing rules, which are still pending, have an opportunity to correct this. The question this article addresses is what that correction should look like.

Part II of this article situates the gig economy in India's legal and economic landscape, with particular attention to the Code on Social Security, 2020 and its partial recognition of gig

[1] The account described is a composite drawn from documented deactivation practices across major Indian food delivery platforms. For documented accounts of platform deactivation in India, see Gig Workers at Risk, India Civil Watch International (2022).

[2] Digital Personal Data Protection Act, No. 22 of 2023 (India). The Act received Presidential assent on August 11, 2023. See Ministry of Electronics and Information Technology, Gazette of India, Aug. 11, 2023.

workers as a distinct legal category. Part III examines algorithmic management as a form of data processing, identifying the specific privacy harms it generates. Part IV analyses the DPDP Act's deemed consent framework and its application, or misapplication, to platform work. Part V addresses the constitutional dimension, drawing on the Supreme Court's right to privacy jurisprudence. Part VI surveys comparative frameworks from the European Union and the United Kingdom. Part VII sets out recommendations for the implementing rules. The article concludes with a brief assessment of what is at stake.

THE GIG ECONOMY IN INDIA: SCALE, STRUCTURE, AND LEGAL STATUS

A. *The Scale of Platform Work*

The gig economy in India has grown at a pace that has significantly outstripped the regulatory frameworks designed to govern it. According to the Niti Aayog's 2022 report on India's Booming Gig and Platform Economy, gig workers constituted approximately 1.5 percent of India's active workforce in 2020-21, with platform-based gig work concentrated in transportation, logistics, food delivery, and domestic services.[3] The report projects this to reach 4.1 percent of the total livelihood workforce by 2029-30, representing 23.5 million workers. These are not marginal figures. They describe a structural transformation of a significant segment of the Indian labour market.

The concentration of gig work in transportation and delivery is particularly significant for data protection purposes. These sectors generate continuous, granular location data as an operational necessity. A delivery worker using a platform application generates location data at intervals of seconds throughout each working hour. Aggregated over a working week, this constitutes a detailed record of the worker's movements, routines, geographic range, and time allocation that is far more comprehensive than the employment records maintained for most formal sector workers.[4]

B. *The Legal Status of Gig Workers*

The most significant legislative development for gig workers in India before the DPDP Act was

[3] See Niti Aayog, India's Booming Gig and Platform Economy: Perspectives and Recommendations on the Future of Work 1, 15 (2022) [hereinafter Niti Aayog Gig Economy Report].
[4] See generally Vili Lehdonvirta, Cloud Empires: How Digital Platforms Are Overtaking the State 87-112 (2022) (describing the surveillance architecture of platform labour markets).

the Code on Social Security, 2020 (the Code). Section 2(35) of the Code defines a gig worker as a person who performs work or participates in a work arrangement and earns from such activities outside of a traditional employer-employee relationship.[5] Section 2(60) defines a platform worker as a person engaged in or undertaking platform work. These definitions created, for the first time, a statutory category for this class of workers distinct from both employees and independent contractors.

The Code's protections for gig and platform workers are, however, limited to social security benefits under Chapter XIII. They do not include the full panoply of employment protections available under the Industrial Disputes Act, 1947, the Factories Act, 1948, or other labour legislation. Critically for present purposes, the Code does not address the data processing that platform companies conduct with respect to their gig workers, nor does it establish any procedural rights in the context of algorithmic management.[6]

Rajasthan enacted the Rajasthan Platform Based Gig Workers (Registration and Welfare) Act, 2023, the first state-level legislation to specifically address the rights of platform gig workers.[7] The Act establishes a Rajasthan Platform Based Gig Workers Welfare Board, provides for a welfare fee levied on platform companies, and requires platforms to establish a grievance redressal mechanism. It does not, however, address algorithmic management practices or the data rights of gig workers in any specific terms.

The Supreme Court has not yet definitively addressed the employment status of gig workers in the platform economy context, though the petition filed by the Indian Federation of App-Based Transport Workers and others, seeking recognition of the employment rights of app-based drivers and delivery workers, remains a significant pending matter.[8] In the absence of a definitive judicial pronouncement, platforms have maintained the contractual position that their workers are independent contractors, and Indian labour authorities have not systematically challenged this characterisation.

[5] Code on Social Security, No. 36 of 2020, s. 2(35) (India) [hereinafter Code on Social Security].
[6] Code on Social Security, ch. XIII, ss. 109-114 (India). See also Kamala Sankaran, Informal Economy, Own-Account Workers and the Law, 33 Indian J.L. & Tech. 1, 14 (2021).
[7] Rajasthan Platform Based Gig Workers (Registration and Welfare) Act, Rajasthan Act No. 9 of 2023 (India).
[8] Indian Fed'n of App-Based Transport Workers v. Union of India, W.P. (C) No. 1071 of 2021 (India) (pending). See also Supriya Routh, App-Based Gig Workers and Labour Rights in India: A Preliminary Assessment, 57 Indian J. Indus. Rel. 437 (2022).

ALGORITHMIC MANAGEMENT: DATA PROCESSING AS LABOUR CONTROL

A. *What Algorithmic Management Does*

The term algorithmic management describes the use of data systems to perform the functions that a human supervisor would traditionally perform: task allocation, performance monitoring, quality assessment, disciplinary action, and work scheduling.[9] In the platform work context, algorithmic management is not a supplement to human management. It is the primary and often sole mechanism through which the platform controls the worker's behaviour.

The data inputs to algorithmic management systems in the Indian gig economy typically include: real-time GPS location data, used for route optimisation and verification of task completion; acceptance and rejection rates, tracking the proportion of assigned tasks that a worker accepts; delivery or ride completion times, measured against platform benchmarks; customer ratings, collected through post-transaction surveys; device usage data, including application usage patterns; and in some platforms, facial recognition data collected at login as an identity verification mechanism.[10]

Each of these data streams is continuously collected, processed through proprietary algorithms whose functioning is not disclosed to workers, and applied to decisions that directly affect the worker's earning capacity. The rating system is the most visible of these decision mechanisms, but it is not the only one. Surge pricing algorithms determine the effective hourly rate that a worker can earn in a given time and location. Task allocation algorithms determine the volume and quality of work available to individual workers. Deactivation algorithms apply threshold conditions that, when triggered, result in the suspension or termination of the worker's access to the platform.

B. *The Privacy Harms of Algorithmic Management*

The privacy harms generated by algorithmic management in the gig economy are qualitatively distinct from the privacy harms that data protection law has historically been most concerned with. They are not primarily harms of disclosure: the location data and performance metrics of

[9] See generally Antonio Aloisi and Valerio De Stefano, Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour 23-56 (2022); Alex Rosenblat, Uberland: How Algorithms Are Rewriting the Rules of Work 3-29 (2018).

[10] *See* Niti Aayog Gig Economy Report, *supra* note 3, at 38-42. *See also* Bama Athreya, *Algorithmic Management and Its Discontents*, 12 Int'l J. Lab. Res. 145 (2021).

a delivery worker are not the kind of information that, if published, would cause the reputational harm associated with sensitive personal data. They are harms of use: the collection and application of this data in ways that determine the worker's livelihood without her knowledge of how the data is being used, without any opportunity to contest the accuracy of the data, and without any procedural mechanism for challenging decisions made on the basis of the data.[11]

These harms have a constitutional dimension that this article addresses in Part V. They also have a specific statutory dimension under the DPDP Act. The Act creates rights of access, correction, and grievance redressal for data principals. Whether these rights are practically meaningful in the algorithmic management context depends on whether the implementing rules require platforms to disclose the data on which algorithmic decisions are based, and whether the grievance redressal mechanism under Section 13 of the Act is accessible to gig workers who, as a practical matter, lack the resources and legal literacy to navigate formal complaint processes.[12]

THE DPDP ACT AND DEEMED CONSENT: A FRAMEWORK UNDER STRAIN

A. *The Deemed Consent Architecture*

The DPDP Act's consent framework is built around two categories. Section 6 governs explicit consent, requiring that it be free, specific, informed, unconditional, and unambiguous, and that it be signified through a clear affirmative action. Section 7 sets out the deemed consent categories, in which processing is treated as lawful without explicit consent because it falls within a closed list of circumstances that the legislature considers sufficient to justify processing without the formality of consent.[13]

Section 7(f) provides that a data fiduciary may process personal data of a data principal for the purpose of employment or for safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, or for performance assessment of the data principal. Section 7(g) extends this to processing that is necessary for the provision of health benefits or

[11] The distinction between disclosure harms and use harms in data protection is developed in Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 507-12 (2006).
[12] Digital Personal Data Protection Act, No. 22 of 2023, ss. 12, 13 (India).
[13] Digital Personal Data Protection Act, No. 22 of 2023, ss. 6, 7 (India).

employment benefits to the data principal.[14]

B. *The Structural Mismatch with Platform Work*

The problem with applying Section 7(f) to gig workers is structural rather than interpretive. The provision was drafted with a conventional employment relationship in mind: an employer processing the personal data of an employee for standard employment management purposes. The data fiduciary in this model is the employer. The data principal is the employee. The processing is for purposes that are reasonably expected in an employment relationship.[15]

Platform gig workers fall outside this model in at least three significant ways. First, they are not employees. The Code on Social Security, 2020 created a distinct statutory category for gig and platform workers precisely because the employment relationship tests under Indian labour law, which typically examine factors such as control, integration, and economic dependence, do not produce a consistent result when applied to platform work. A deemed consent provision framed in terms of employment processing does not straightforwardly apply to a relationship that is not legally characterised as employment.

Second, even if Section 7(f) is interpreted broadly to encompass platform work arrangements, the scope of processing that platforms actually conduct goes well beyond what a conventional employment deemed consent framework would cover. Continuous location tracking at second-level intervals, the collection of facial recognition data for identity verification, the construction of behavioural profiles through the aggregation of acceptance rates and delivery times, and the use of machine learning models to generate predictive assessments of worker reliability are not processing activities that fall naturally within the concept of performance assessment as understood in a conventional employment context.[16]

Third, the deemed consent framework carries no procedural protections for the data principal in the context of adverse decisions. In a conventional employment relationship, an employee whose employment is terminated has recourse to industrial dispute mechanisms, standing orders, and natural justice protections that require the employer to provide reasons and an

[14] Digital Personal Data Protection Act, No. 22 of 2023, ss. 7(f), 7(g) (India).
[15] *See* Usha Ramanathan, *A Illegitimate Law?*, Econ. & Pol. Wkly., Oct. 7, 2023, at 10 (critiquing the DPDP Act's deemed consent provisions as insufficiently tailored to specific categories of vulnerable data principals).
[16] For the specific data processing architecture of Indian food delivery and ride-hailing platforms, see *Understanding Platform Data Practices in India*, IT for Change Policy Brief No. 7 (2022).

opportunity to be heard. Gig workers, who are not employees, have none of these protections. When an algorithmic system applies a threshold and deactivates a worker's account, the DPDP Act as currently drafted provides the worker with a right to access her personal data and to file a complaint with the Data Protection Board, but does not require the platform to explain how the data was used or what the basis of the deactivation decision was.[17]

C. *The Notice Failure*

Section 5 of the DPDP Act requires that a data fiduciary give the data principal notice of the personal data to be processed and the purposes of processing before seeking consent. Where deemed consent applies, the notice obligation exists but is uncoupled from any consent transaction. A platform company's privacy policy, presented to a gig worker on a mobile device at the point of registration, constitutes the notice on which the deemed consent framework rests.[18]

The practical adequacy of this notice is deeply questionable. Research on the readability of privacy policies in Indian languages has consistently found that the documents are written at a comprehension level significantly above the educational attainment of the populations most heavily engaged in gig work.[19] The workers who are most exposed to the harms of algorithmic management are those least able to understand the data processing framework under which they operate. A deemed consent architecture that depends on notice as its primary legitimising mechanism must grapple with this asymmetry.

THE CONSTITUTIONAL DIMENSION: PRIVACY, DIGNITY, AND ALGORITHMIC ACCOUNTABILITY

A. *The Right to Privacy and Informational Self-Determination*

The Supreme Court's decision in K.S. Puttaswamy (Retd.) v. Union of India established the right to privacy as a fundamental right under Article 21 of the Constitution of India.[20] The

[17] Digital Personal Data Protection Act, No. 22 of 2023, s. 13 (India). *Cf.* Industrial Disputes Act, No. 14 of 1947, s. 11A (India) (conferring on labour tribunals the power to assess the proportionality of dismissal orders).
[18] Digital Personal Data Protection Act, No. 22 of 2023, s. 5 (India).
[19] *See* Sunil Abraham and Sumandro Chattapadhyay, *Privacy and the People: A Framework for Civil Society Engagement on Data Protection in India*, Centre for Internet and Society Working Paper 14 (2018).
[20] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter *Puttaswamy*]. The nine-judge bench decision was unanimous in holding that the right to privacy is a fundamental right under the Constitution of India, though individual justices articulated the scope and content of the right differently.

majority judgment, authored by Justice D.Y. Chandrachud (as he then was), articulated privacy as encompassing three distinct dimensions: spatial privacy (protection of the body and the home), decisional privacy (protection of autonomous personal choices), and informational privacy (protection of personal information from collection, use, and disclosure).

The informational privacy strand of Puttaswamy is directly relevant to algorithmic management in the gig economy. The Court held that the right to privacy protects individuals against the use of personal information as an instrument of surveillance and control.[21] The continuous collection of location data, behavioural metrics, and performance indicators by platform companies, and the application of this data through opaque algorithmic systems to decisions that determine a worker's ability to earn a livelihood, falls squarely within the kind of informational surveillance that the Court identified as constitutionally significant.

The Court in Puttaswamy also engaged with the concept of contextual integrity, drawing on the work of Helen Nissenbaum, to articulate the proposition that information flows appropriately when they match the norms of the context in which information was originally shared.[22] A gig worker who shares her location data for the purpose of receiving task assignments does not, by that act, consent to the construction of a comprehensive behavioural profile that is used to make predictive assessments of her reliability or to calibrate the difficulty of the tasks she is offered. The contextual norm of location sharing for task completion does not encompass these downstream uses.

B. *The Right to Livelihood and Natural Justice*

The Supreme Court in Olga Tellis v. Bombay Municipal Corporation recognised the right to livelihood as a component of the right to life under Article 21.[23] The Court held that the right to life does not mean merely the right to animal existence but includes the right to earn a livelihood. The deactivation of a gig worker from a platform, where the platform is her primary or sole source of income, implicates the right to livelihood in a way that engages the procedural

[21] Puttaswamy, (2017) 10 SCC 1, at 471 (Chandrachud, J.) ('Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the State but from non-State actors as well.') (India).
[22] Puttaswamy, (2017) 10 SCC 1, at 469 (citing Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2009)) (India).
[23] Olga Tellis v. Bombay Mun. Corp., (1985) 3 SCC 545, at para. 32 (India) ('The right to life includes the right to livelihood. The sweep of the right to life conferred by Art. 21 is wide and far reaching.').

protections of Article 21.

The right to be heard before an adverse decision is made, a fundamental principle of natural justice, has been consistently applied by Indian courts in contexts where a person's livelihood is at stake. In Maneka Gandhi v. Union of India, the Supreme Court held that any procedure affecting a fundamental right must be fair, just, and reasonable.[24] An algorithmic deactivation process that provides no explanation of the basis of the decision, no opportunity to contest the factual inputs, and no meaningful internal review mechanism does not meet this standard, particularly when the right to livelihood under Article 21 is engaged.

It is true that the application of constitutional natural justice principles to private platform companies is doctrinally contested. Article 21 operates against the State, and private companies are not State actors in the ordinary constitutional sense. However, the Supreme Court's decision in Zee Telefilms Ltd. v. Union of India recognised that bodies exercising public functions may be subject to constitutional obligations even where they are not formally part of the State.[25] The argument that platform companies exercising effective monopoly control over workers' access to income perform a quasi-public function is one that Indian courts have not yet had to resolve, but which the pending petition before the Supreme Court may require them to address.

COMPARATIVE PERSPECTIVES: THE EU AND UK APPROACHES

A. *The EU Platform Work Directive*

The European Union's Directive on Improving Working Conditions in Platform Work (the Platform Work Directive), which entered into force in December 2024, represents the most comprehensive legislative response to the specific challenges of platform work anywhere in the world.[26] The Directive creates a legal presumption of employment for platform workers, reversible by the platform on proof that a genuine independent contractor relationship exists. It also includes specific provisions on algorithmic management that are directly relevant to the Indian context.

[24] Maneka Gandhi v. Union of India, (1978) 1 SCC 248, at para. 56 (India) (holding that any procedure under Article 21 'must be right, just and fair and not arbitrary, fanciful or oppressive').
[25] Zee Telefilms Ltd. v. Union of India, (2005) 4 SCC 649 (India) (examining the conditions under which a private body exercising public functions may be subject to writ jurisdiction).
[26] Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work, 2024 O.J. (L 2024/2831) [hereinafter Platform Work Directive].

Article 9 of the Platform Work Directive requires platform companies to provide information to workers about the automated monitoring and decision-making systems that affect them. Article 10 requires human review of significant decisions made by automated systems, including deactivation decisions. Article 11 prohibits platform companies from collecting personal data through automated monitoring except where the data is necessary for the performance of the contract.[27] Taken together, these provisions create a framework of algorithmic accountability that the DPDP Act's deemed consent provisions do not replicate.

The Directive's algorithmic accountability framework rests on a logic that is consistent with the informational privacy principles articulated in Puttaswamy: where automated systems make decisions that affect workers' livelihoods, those workers are entitled to understand the basis of those decisions and to have access to a human decision-maker. This is not a radical principle. It is the data protection analogue of the natural justice requirements that Indian employment law has long applied to disciplinary proceedings.

B. *The UK Supreme Court in Uber BV v. Aslam*

The United Kingdom Supreme Court's unanimous decision in Uber BV v. Aslam is the most significant judicial treatment of gig worker status in any common law jurisdiction.[28] The Court held that Uber drivers were workers within the meaning of the Employment Rights Act, 1996, entitling them to minimum wage guarantees, paid holiday, and whistleblower protections. The Court rejected Uber's characterisation of its drivers as independent contractors operating a business through the Uber platform.

The Court's reasoning is relevant to the DPDP Act analysis for two reasons. First, the Court's identification of the indicia of control that establish the worker relationship, including the setting of fares, the management of the customer relationship, the imposition of performance standards, and the unilateral power to deactivate drivers, are precisely the functions performed by algorithmic management systems in Indian platforms.[29] Second, the Court's recognition that the formal contractual characterisation of the relationship as one of independent contract does not preclude a more realistic assessment of the actual relationship has implications for how

[27] Platform Work Directive, arts. 9-11.
[28] Uber BV v. Aslam [2021] UKSC 5 (appeal taken from [2019] EWCA Civ 3 (Eng.)).
[29] Uber BV v. Aslam [2021] UKSC 5, para. 94 (Lord Leggatt JSC) ('Uber exercises a high degree of control over the way in which drivers deliver their services.').

Indian courts and regulators might approach the Section 7(f) deemed consent question.

If the functional indicia of the platform relationship establish sufficient control to constitute employment for labour law purposes, there is a strong argument that the deemed consent provisions designed for employment contexts should apply to that relationship. The corollary, however, is that the procedural protections that employment law attaches to employment relationships, including protection against arbitrary termination and the right to reasons for adverse decisions, should also apply. The Uber BV logic cuts both ways.[30]

C. *The United States: Algorithmic Transparency and State-Level Approaches*

In the United States, the algorithmic management question has been approached primarily through state-level legislation and sectoral regulation. The California Supreme Court's decision in Dynamex Operations West, Inc. v. Superior Court established an ABC test for classifying workers as employees, requiring employers to establish that a worker performs work outside the usual course of the hiring entity's business before classifying them as an independent contractor.[31] California's Assembly Bill 5, enacted in 2019, codified the Dynamex standard, though Proposition 22, passed by California voters in 2020, created a specific exception for app-based transportation and delivery companies.

At the federal level, the Federal Trade Commission has increasingly applied consumer protection principles to algorithmic management practices, particularly in the context of dark patterns and deceptive design. The National Labor Relations Board under General Counsel Jennifer Abruzzo issued a 2022 memorandum identifying algorithmic control as potentially relevant to the determination of employee status under the National Labor Relations Act.[32] These developments reflect a growing recognition in the United States that the data processing dimensions of algorithmic management require regulatory attention distinct from, but connected to, the labour law classification question.

---

[30] *Cf.* Jeremias Prassl, *Humans as a Service: The Promise and Perils of Work in the Gig Economy* 71-95 (2018) (arguing that the economic and regulatory consequences of platform work classification should follow the functional reality of the relationship).

[31] Dynamex Operations W., Inc. v. Superior Court, 416 P.3d 1 (Cal. 2018).

[32] National Labor Relations Board, Office of the General Counsel, Memorandum GC 22-04, Analysis of the Application of *Amazon Flex* Algorithm to Determine Whether an Employer Is Entitled to NLRA Coverage (2022).

RECOMMENDATIONS FOR THE DPDP IMPLEMENTING RULES

A. *Gig Worker-Specific Deemed Consent Schedule*

The implementing rules under Section 7 should include a specific schedule addressing the processing of personal data of platform gig workers. This schedule should: first, confirm that the deemed consent provisions of Section 7(f) apply to platform work arrangements as defined under the Code on Social Security, 2020, regardless of whether the relationship is formally characterised as employment; second, enumerate the categories of processing that are covered by deemed consent in the platform work context, distinguishing between processing that is operationally necessary for task allocation, which should be covered, and processing for secondary purposes such as behavioural profiling and creditworthiness assessment, which should require explicit consent; and third, specify the minimum notice obligations that apply to platform companies in communicating their data processing practices to gig workers in languages and formats accessible to the workers who use their platforms.[33]

B. *A Mandatory Explainability Requirement for Deactivation*

The rules should create a specific obligation on data fiduciaries operating platform work arrangements to provide a written explanation of the basis of any automated decision that results in the suspension or termination of a gig worker's access to the platform. This explanation should identify: the data inputs that contributed to the decision, the threshold or condition that triggered the decision, and the process by which the worker may seek human review of the automated decision. This requirement should be implemented through the grievance redressal mechanism under Section 13 of the Act, with the Data Protection Board empowered to direct reinstatement of access pending review in cases where the platform cannot demonstrate compliance.[34]

This recommendation is consistent with the approach taken in Article 10 of the EU Platform Work Directive and with the natural justice principles that Indian courts have applied to adverse decisions affecting livelihood. It does not require platforms to disclose proprietary algorithmic code. It requires them to explain, in human-intelligible terms, why a specific decision was made

[33] *See* Code on Social Security, No. 36 of 2020, ss. 2(35), 2(60), ch. XIII (India) (providing the definitional basis for a gig worker-specific DPDP rule schedule).
[34] Digital Personal Data Protection Act, No. 22 of 2023, s. 13 (India). *Cf.* Platform Work Directive, art. 10 (requiring human review of algorithmic decisions affecting platform workers in the EU).

about a specific worker. This is a reasonable standard.

C. *A Data Minimisation Standard for Algorithmic Management*

The implementing rules should specify data minimisation standards applicable to the algorithmic management context. The DPDP Act's Section 6(1) requires that consent be sought for a specific purpose and that processing be limited to data necessary for that purpose. Section 7 deemed consent should carry an equivalent minimisation obligation. Rules should specify that continuous location tracking is permissible only during active task performance, that facial recognition data collected for identity verification may not be retained beyond the verification event, and that behavioural data collected for one purpose, such as fraud detection, may not be repurposed for secondary algorithmic assessments such as reliability scoring without separate authorisation.[35]

CONCLUSION

The gig worker deactivated from a delivery platform in Mumbai is, in the language of data protection law, a data principal. She has rights. She can access her personal data. She can file a complaint with the Data Protection Board. She can, theoretically, withdraw consent to processing, though the practical consequence of doing so is that she loses access to her source of income.

These rights exist on paper. They do not, as the DPDP Act is currently structured, translate into meaningful protection against the specific harms that algorithmic management generates. The deemed consent framework, designed for a conventional employment relationship, does not fit the platform work context. The notice framework, built around written privacy policies, does not function in a population characterised by linguistic diversity and constrained digital literacy. The grievance redressal mechanism, absent specific rules on algorithmic accountability, does not provide a practical remedy for arbitrary deactivation.[36]

The implementing rules are the mechanism through which these failures can be corrected without legislative amendment. The Code on Social Security, 2020 recognised gig workers as

[35] Digital Personal Data Protection Act, No. 22 of 2023, s. 6(1) (India). *See also* Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 141-88 (2015).
[36] Puttaswamy, (2017) 10 SCC 1, at 265 (Kaul, J.) ('Privacy of the individual is an essential aspect of dignity. Dignity has both an intrinsic and instrumental value.') (India).

a distinct legal category deserving specific attention. The DPDP rules should do the same.

The Supreme Court in Puttaswamy described privacy as a tool that allows individuals to develop thoughts without external interference, to have a private space for their beliefs and to negotiate their own identity. For a gig worker whose every working moment is tracked, rated, and algorithmically assessed, this description of privacy as space for self-determination has an almost ironic quality. The law's task is to make it less ironic. The rules are where that work must begin.

BIBLIOGRAPHY

I. **Primary Sources**

A. **Constitutional Provisions**

Constitution of India, arts. 14, 19, 21

B. **Legislation**

a) Digital Personal Data Protection Act, No. 22 of 2023 (India)

b) Code on Social Security, No. 36 of 2020 (India)

c) Industrial Disputes Act, No. 14 of 1947 (India)

d) Information Technology Act, No. 21 of 2000 (India)

e) Rajasthan Platform Based Gig Workers (Registration and Welfare) Act, No. 9 of 2023 (India)

f) Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on Improving Working Conditions in Platform Work

g) Employment Rights Act, 1996 (U.K.)

h) California Assembly Bill 5, Stats. 2019, ch. 296 (Cal.)

C. **Cases**

a) Indian Fed'n of App-Based Transport Workers v. Union of India, W.P. (C) No. 1071 of 2021 (India) (pending)

b) K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)

c) Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India)

d) Olga Tellis v. Bombay Mun. Corp., (1985) 3 SCC 545 (India)

e) Zee Telefilms Ltd. v. Union of India, (2005) 4 SCC 649 (India)

f) Dynamex Operations W., Inc. v. Superior Court, 416 P.3d 1 (Cal. 2018)

g) Uber BV v. Aslam [2021] UKSC 5

II. Secondary Sources

A. Books

a) Aloisi, Antonio and Valerio De Stefano, Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour (Hart Publishing, 2022)

b) Lehdonvirta, Vili, Cloud Empires: How Digital Platforms Are Overtaking the State (MIT Press, 2022)

c) Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, 2009)

d) Pasquale, Frank, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, 2015)

e) Prassl, Jeremias, Humans as a Service: The Promise and Perils of Work in the Gig Economy (Oxford University Press, 2018)

f) Rosenblat, Alex, Uberland: How Algorithms Are Rewriting the Rules of Work (University of California Press, 2018)

B. Articles

a) Athreya, Bama, Algorithmic Management and Its Discontents, 12 Int'l J. Lab. Res. 145 (2021)

b) Routh, Supriya, App-Based Gig Workers and Labour Rights in India: A Preliminary Assessment, 57 Indian J. Indus. Rel. 437 (2022)

c) Sankaran, Kamala, Informal Economy, Own-Account Workers and the Law, 33 Indian J.L. & Tech. 1 (2021)

d) Solove, Daniel J., A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006)

C. **Reports and Working Papers**

a) Niti Aayog, India's Booming Gig and Platform Economy: Perspectives and Recommendations on the Future of Work (2022)

b) IT for Change, Understanding Platform Data Practices in India, Policy Brief No. 7 (2022)

c) National Labor Relations Board, Office of General Counsel, Memorandum GC 22-04 (2022)