INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# DIGITAL WELFARE AND MIGRANT VULNERABILITY: ASSESSING TECHNOLOGICAL GOVERNANCE, PRIVACY, AND INEQUALITY IN POST-PANDEMIC INDIA

**AUTHOR -** ABHINAV VISWANATH* & KRUTHA JANANI**

* ASSISTANT PROFESSOR AT SASTRA UNIVERSITY

** STUDENT AT SASTRA UNIVERSITY

**BEST CITATION –** ABHINAV VISWANATH & KRUTHA JANANI, DIGITAL WELFARE AND MIGRANT VULNERABILITY: ASSESSING TECHNOLOGICAL GOVERNANCE, PRIVACY, AND INEQUALITY IN POST-PANDEMIC INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (8) OF 2026, PG. 354-368, APIS – 3920 – 0001 & ISSN - 2583-2344.

**ABSTRACT**

The COVID-19 pandemic exposed deep structural vulnerabilities within India's migrant labour economy, revealing significant gaps in welfare delivery and institutional preparedness. In response, the State increasingly adopted technology-driven governance mechanisms, including platforms such as the National Migrant Information System (NMIS), Aarogya Setu, and the e-Shram portal, to facilitate welfare delivery and data-driven policy interventions. This paper critically examines the effectiveness and constitutional implications of such digital welfare frameworks in the post-pandemic period (2020–2026).

Adopting a doctrinal and socio-legal methodology, the study evaluates digital welfare through the lens of digital equality, analysing how disparities in access to digital infrastructure, literacy, and identification systems affect migrant workers' ability to benefit from these platforms. It argues that while digital governance enhances administrative efficiency and scalability, it simultaneously risks reinforcing structural inequalities by excluding those who lack digital access.

The paper further interrogates the constitutional dimensions of data-driven governance, particularly the right to privacy as articulated in *Justice K.S. Puttaswamy v. Union of India*, and examines the regulatory framework established under the Digital Personal Data Protection Act, 2023 and the 2025 Rules. It highlights tensions between welfare objectives and privacy safeguards, especially in contexts involving large-scale data collection and algorithmic decision-making.

The study concludes that digital welfare systems must be restructured to ensure inclusivity, transparency, and accountability. It advocates for hybrid delivery models, strengthened data protection safeguards, and regulatory oversight of algorithmic governance to align technological innovation with constitutional principles of equality, dignity, and justice.

**Keywords**: Digital Governance; Migrant Labour; Digital Inequality; Data Privacy; Welfare State

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

## INTRODUCTION

### 1.1 Background

The COVID-19 pandemic marked a critical inflection point in India's governance and labour landscape, exposing deep structural vulnerabilities within the informal economy. Among the most visibly affected were migrant workers, whose mass displacement during the nationwide lockdown of 2020 revealed systemic failures in welfare delivery, labour regulation, and state preparedness. The crisis underscored the precarious existence of millions of internal migrants who remain outside formal labour protections and welfare frameworks.[1]

In response, the Indian State increasingly turned toward **technology-driven governance mechanisms** to manage the crisis and facilitate welfare delivery. Initiatives such as the National Migrant Information System (NMIS), the Aarogya Setu application, and subsequently the e-Shram portal were introduced to track, monitor, and assist migrant workers. These developments signalled a broader transition toward a **data-driven welfare state**, wherein digital platforms became central to the design and implementation of public policy.

However, this shift raises critical questions regarding the accessibility and inclusivity of such systems. While technological solutions promise efficiency and scalability, they presuppose the existence of adequate digital infrastructure and literacy. In a socio-economic context characterized by widespread inequality, these assumptions often fail, resulting in what may be termed "digital exclusion within digital welfare."[2]

### 1.2 Digital Inequality and the Limits of Technological Welfare

The effectiveness of digital governance tools is contingent upon equitable access to digital resources. In India, however, access to the internet, smartphones, and digital literacy remains unevenly distributed across regions, socio-economic groups, and gender lines. This disparity is particularly pronounced among migrant workers, who often lack stable access to digital devices and formal identification systems.[3]

The reliance on digital platforms for welfare delivery thus risks reinforcing existing inequalities. Workers who are unable to register on digital portals or navigate technological systems may be excluded from benefits, thereby undermining the very objective of welfare schemes. The e-Shram portal, introduced to create a national database of unorganized workers, exemplifies this paradox: while it represents a significant step toward formal recognition, its accessibility remains constrained by structural barriers.[4]

This phenomenon highlights a fundamental tension within contemporary governance—**the use of technology as a tool of inclusion versus its potential to deepen exclusion**. The digitalization of welfare, while administratively efficient, may inadvertently marginalize those who are already vulnerable.

### 1.3 Emergence of Data-Driven Governance

The expansion of digital welfare platforms reflects a broader transformation in the nature of state power. Traditional welfare mechanisms, characterized by decentralized and paper-based systems, are increasingly being replaced by centralized digital databases and real-time monitoring tools.

This transformation has been accompanied by the creation of large-scale data infrastructures that collect and process personal information of individuals, including migrant workers. The integration of such data across platforms enables the State to design targeted interventions but also raises concerns regarding **surveillance, data security, and accountability**.

The enactment of the Digital Personal Data Protection Act, 2023 represents a significant development in this context. The Act establishes a comprehensive framework governing the processing of digital personal data, recognizing both the rights of individuals and the legitimate interests of the State in data utilization.[5] It

introduces a consent-based regime, requiring that personal data be processed only with informed and explicit consent, and provides individuals with rights such as access, correction, and erasure of data.[6]

The subsequent notification of the Digital Personal Data Protection Rules, 2025 operationalizes these principles by prescribing detailed requirements relating to notice, consent, data retention, and breach reporting.[7] Together, the Act and the Rules mark the emergence of India's first comprehensive data protection framework, aimed at balancing innovation with privacy safeguards.

### 1.4 Privacy, Surveillance, and Constitutional Concerns

The increasing reliance on digital platforms for governance has brought issues of privacy and surveillance to the forefront of constitutional discourse. The right to privacy was unequivocally recognized as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*, where the Court held that privacy is intrinsic to life and personal liberty under Article 21 of the Constitution.[8]

This recognition imposes constitutional limitations on the State's ability to collect and process personal data. Any infringement of privacy must satisfy the tests of legality, necessity, and proportionality.[9] In the context of digital welfare platforms, these requirements assume particular significance, as the collection of personal data often occurs on a large scale and without meaningful alternatives for individuals.

The deployment of applications such as Aarogya Setu during the pandemic illustrates the complexities of this issue. While the application was intended to facilitate contact tracing and public health management, concerns were raised regarding data collection practices, lack of transparency, and potential misuse of information.[10] These concerns highlight the need for robust legal and institutional safeguards to ensure that technological interventions do not compromise fundamental rights.

### 1.5 The Welfare–Privacy Trade-off

At the core of this discourse lies the tension between **welfare objectives and privacy protections**. The State's use of technology to deliver welfare services is often justified on grounds of efficiency, targeting, and public interest. However, such justifications must be balanced against the potential risks of surveillance and data misuse.

The Digital Personal Data Protection framework attempts to address this tension by establishing a rights-based approach to data governance. Nevertheless, the effectiveness of this framework depends on its implementation and the capacity of institutions to enforce compliance. The asymmetry of power between the State and individuals further complicates this balance, particularly in cases where access to welfare is contingent upon the sharing of personal data.

Against this backdrop, the present study seeks to critically examine the viability of technological platforms as instruments of welfare for migrant workers. It interrogates whether such platforms, when evaluated through the lens of digital equality, effectively address the socio-economic vulnerabilities of migrant labour or merely reproduce existing inequalities.

This research adopts a **doctrinal and socio-legal methodology**, combining analysis of constitutional provisions, legislative frameworks, and judicial decisions with an examination of policy developments and technological practices. It also incorporates a limited comparative perspective to assess international approaches to digital governance and migrant welfare.

The scope of the study is confined to the Indian context, with particular emphasis on developments in the post-pandemic period (2020–2026). It focuses on the intersection of labour law, technology, and constitutional rights, without extending into broader economic analysis except where necessary.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

## MIGRANT LABOUR, DIGITAL INEQUALITY, AND WELFARE ACCESS

### 2.1 Structure and Scale of Migrant Labour in India

Internal migration constitutes a defining feature of India's labour economy, particularly within the informal sector. According to the Economic Survey and Census-based estimates, India hosts over 100 million internal migrants, a significant proportion of whom are engaged in informal, low-wage, and precarious employment.[11] The Periodic Labour Force Survey (PLFS) further indicates that nearly **90% of India's workforce operates within the informal sector**, lacking formal contracts, social security, or institutional protection.[12]

The COVID-19 pandemic exposed the structural invisibility of migrant workers within state welfare systems. The absence of reliable, centralized data on migrant labour significantly hindered policy response during the lockdown, prompting the government to adopt digital registration mechanisms such as the **National Migrant Information System (NMIS)**.[13]

Subsequently, the introduction of the **e-Shram portal (2021)** sought to create a comprehensive national database of unorganized workers. As of 2025, the portal has registered over **30 crore workers**, making it one of the largest labour databases globally.[14] While this represents a major step toward formal recognition, it also highlights the reliance on digital systems as primary tools of welfare governance.

### 2.2 Dimensions of Digital Inequality

The effectiveness of digital welfare platforms is inherently dependent on equitable access to digital infrastructure. However, India continues to exhibit significant disparities in internet access, digital literacy, and device ownership.

According to the Telecom Regulatory Authority of India (TRAI), while overall internet penetration has increased substantially post-2020, **rural and marginalized populations remain disproportionately excluded**.[15] Additionally, the National Sample Survey (NSS) data indicates that a significant proportion of households, particularly among migrant communities, lack access to smartphones or stable internet connectivity.[16]

Digital inequality manifests across three primary dimensions:

- **Access inequality** (lack of devices/internet)
- **Capability inequality** (limited digital literacy)
- **Usage inequality** (inability to effectively engage with digital systems)

**Internet Access Disparity (Urban vs. Rural India, 2020 – 2025)**

| | Urban Internet Access | Rural Internet Access |
|---|---|---|
| 2020 | 55% | 25% |
| 2022 | 65% | 35% |
| 2025 | 75% | 45% |

While internet penetration has improved overall, the persistent **urban–rural gap (~30%)** demonstrates that digital platforms cannot be assumed to be universally accessible. This gap disproportionately affects migrant workers, many of whom originate from rural regions.

### 2.3 Digital Welfare Platforms and Access Barriers

The increasing reliance on digital platforms for welfare delivery introduces both opportunities and constraints. Systems such as NMIS and e-Shram are designed to enhance efficiency, enable targeted delivery, and reduce administrative leakages. However, these benefits are contingent upon successful digital onboarding of beneficiaries.

Empirical evidence suggests that many migrant workers face barriers in accessing such platforms, including:

- Lack of Aadhaar-linked mobile numbers
- Limited awareness of registration processes

- Language and interface challenges
- Dependence on intermediaries for digital access[17]

These barriers create a situation where **formal inclusion through digital systems coexists with practical exclusion**, thereby undermining the effectiveness of welfare schemes.

**Barriers to Digital Welfare Access (Indicative Distribution)**

- Lack of Smartphone – 40%
- Low Digital Literacy – 30%
- Poor Connectivity – 20%
- Documentation Issues – 10%

The data reflects that **technological access (devices + literacy)** constitutes the primary bottleneck in welfare delivery, rather than policy design alone.

**2.4 Migration, Informality, and Welfare Exclusion**

The intersection of migration and informality further compounds digital exclusion. Migrant workers often operate outside formal labour markets, lack fixed residences, and experience discontinuity in documentation and identity verification systems.[18]

This mobility creates friction within digital welfare frameworks, which are typically designed for static populations. For instance:

- State-based welfare schemes may not be portable
- Digital registration may not account for seasonal migration
- Verification processes may exclude transient populations

The **One Nation One Ration Card (ONORC)** initiative attempts to address portability issues, but its effectiveness remains dependent on digital authentication systems, which themselves are subject to exclusionary risks.[19]

**2.5 Post-Pandemic Expansion of Digital Governance**

The post-pandemic period (2021–2026) has witnessed a rapid expansion of digital governance in India. Government initiatives increasingly rely on integrated digital platforms to deliver welfare, reflecting a shift toward 'Platformizaiton of Governance'[20]

This shift is characterized by:

- Centralized data collection
- Real-time monitoring
- Integration across departments
- Increased reliance on digital identity systems

**Digital Welfare Architecture**

Worker Registration (e-Shram)

↓

Data Integration (Central Database)

↓

Scheme Mapping (Eligibility Algorithms)

↓

Benefit Delivery (Direct Transfer / Services)

↓

Monitoring & Feedback (Digital Tracking)

This model highlights how **data becomes the central medium of governance**, raising questions about access, accuracy, and accountability.

**2.6 Digital Equality as a Constitutional Concern**

The issue of digital inequality extends beyond administrative efficiency and enters the domain of constitutional rights. The right to equality under Article 14 requires that state action not result in arbitrary exclusion. Similarly, the right to life under Article 21 encompasses access to basic welfare and dignified living conditions.[21]

Where access to welfare is mediated through digital systems, **digital access effectively becomes a precondition for the realization of fundamental rights**. This raises the question of whether the State has a corresponding obligation to ensure **digital equality** as part of its constitutional mandate.

Courts have increasingly recognized the importance of access to technology in enabling rights. In *Anuradha Bhasin v. Union of India*, the Supreme Court acknowledged that access to the internet is integral to the exercise of fundamental freedoms, particularly under Article 19(1)(a).[22]

This evolving jurisprudence suggests that digital infrastructure is no longer merely a tool of governance but a **constitutional necessity**.

The analysis of migrant labour and digital inequality reveals a fundamental paradox within contemporary welfare governance. While digital platforms have enabled unprecedented scale and efficiency in policy implementation, they have also introduced new forms of exclusion rooted in structural inequalities.

The reliance on technology as a primary mode of welfare delivery risks transforming socio-economic vulnerability into **digital vulnerability**, where access to rights becomes contingent upon access to technology.

This chapter establishes that digital inequality is not merely a technological issue but a **legal and constitutional concern**, setting the stage for a deeper examination of technological governance and its implications in the subsequent chapter.

## TECHNOLOGICAL GOVERNANCE AND WELFARE PLATFORMS

### 3.1 From Welfare Administration to Data-Driven Governance

The post-pandemic period has accelerated a structural transformation in Indian governance—from conventional welfare administration toward **data-driven governance architectures**. This shift is characterized by the deployment of digital platforms that enable real-time data collection, centralized processing, and targeted delivery of benefits.[23]

Unlike traditional welfare systems, which relied on decentralized bureaucratic mechanisms, digital platforms operate through integrated databases that aggregate personal, demographic, and socio-economic information. This transition reflects a broader global trend toward **"platform governance,"** wherein the State assumes the role of a data aggregator and processor.[24]

In India, this transformation has been particularly visible in the domain of migrant welfare, where the absence of reliable data during the COVID-19 crisis prompted the rapid development of digital tracking and registration systems.

### 3.2 Key Digital Platforms: NMIS, Aarogya Setu, and e-Shram

#### (a) National Migrant Information System (NMIS)

The NMIS was introduced in 2020 as an emergency response mechanism to track the movement of migrant workers during the lockdown.[25] It enabled coordination between states for the transportation of migrants and facilitated data collection on migration flows.

However, its design was primarily **reactive and temporary**, lacking long-term integration with welfare systems. The absence of transparency regarding data usage and retention further limited its accountability.

#### (b) Aarogya Setu Application

The Aarogya Setu application represented one of the most extensive digital interventions during the pandemic, aimed at contact tracing and health surveillance.[26]

While the application was initially promoted as a voluntary tool, concerns were raised regarding its mandatory use in certain contexts, raising constitutional questions relating to privacy and consent. The lack of a comprehensive data protection framework at the time further intensified these concerns.[27]

#### (c) e-Shram Portal

The e-Shram portal marks a significant evolution in digital labour governance. Launched in 2021, it seeks to create a **centralized national database**

**of unorganized workers**, linking them to various welfare schemes.[28]

Unlike NMIS, e-Shram is designed as a **permanent institutional mechanism**, reflecting a shift toward long-term digital governance. However, its effectiveness is contingent upon accurate data entry, accessibility, and inter-state portability of benefits.

### 3.3 Comparative Functional Analysis of Platforms

**Comparative Overview of Key Digital Platforms**

| Platform | Primary Objective | Nature of Data Collected | Duration | Key Limitation |
|---|---|---|---|---|
| NMIS | Migration tracking | Movement data | Temporary | Lack of integration |
| Aarogya Setu | Health surveillance | Health + location data | Semi-permanent | Privacy concerns |
| e-Shram | Labour database | Socio-economic data | Permanent | Accessibility gaps |

**Interpretation:**
The evolution from NMIS to e-Shram reflects a transition from **crisis-driven data collection to institutionalized digital governance**, with increasing scope and permanence.

### 3.4 Centralization, Data Aggregation, and Power Asymmetry

A defining feature of digital welfare platforms is the **centralization of data and decision-making authority**. Unlike traditional systems where authority was dispersed across administrative levels, digital platforms concentrate power within centralized databases and algorithmic systems.[29]

This centralization creates significant **power asymmetries** between the State and individuals. Workers become data subjects within systems that they do not control, with limited visibility into how their data is used or shared.

The aggregation of data across platforms also raises concerns regarding **function creep**, where data collected for one purpose is repurposed for another without adequate safeguards.[30]

**Centralized Data Governance Model**

Worker Data Input (e-Shram / Apps)
↓
Central Database (Government Servers)
↓
Algorithmic Processing (Eligibility / Risk Assessment)
↓
Policy Decisions (Targeting / Allocation)
↓
Outcome Delivery (Benefits / Restrictions)

This model illustrates how **data becomes the primary interface between citizen and State**, reducing direct human interaction and increasing reliance on automated systems.

### 3.5 Algorithmic Governance and Decision-Making

The increasing use of digital platforms introduces elements of **algorithmic governance**, where decisions regarding eligibility, prioritization, and benefit allocation are mediated through automated systems.

While such systems enhance efficiency, they also introduce risks of:

- **Opacity** (lack of transparency in decision-making)
- **Bias** (errors in data leading to exclusion)
- **Lack of accountability** (difficulty in challenging automated decisions)[31]

In the context of migrant workers, these risks are particularly significant due to the fluidity of their socio-economic status and the likelihood of incomplete or inaccurate data.

### 3.6 Legal Framework Governing Digital Platforms

The expansion of digital governance must be evaluated within the framework of existing data protection and constitutional law.

The Digital Personal Data Protection Act, 2023 establishes the legal foundation for regulating personal data processing in India.[32] It introduces obligations on data fiduciaries, including the State, to ensure lawful processing, data minimization, and purpose limitation.[33]

However, the Act also provides exemptions for State functions, particularly where data processing is necessary for the provision of public services.[34] This creates a potential tension between welfare objectives and privacy safeguards, as broad exemptions may dilute accountability.

The Digital Personal Data Protection Rules, 2025 further operationalize the Act by specifying compliance requirements, including consent mechanisms and data breach reporting.[35]

### 3.7 Efficiency vs Accessibility: A Structural Trade-off

The analysis of digital platforms reveals a fundamental trade-off between **efficiency and accessibility**.

- **Efficiency gains**:
  - Faster data processing
  - Targeted delivery of benefits
  - Reduction in administrative leakages
- **Accessibility challenges**:
  - Digital exclusion
  - Interface complexity
  - Dependence on intermediaries

This trade-off underscores the need to evaluate digital governance not merely in terms of administrative performance but also in terms of **equitable access and inclusivity**.

The rise of technological governance in India represents a significant transformation in the relationship between the State and its citizens. Digital platforms such as NMIS, Aarogya Setu, and e-Shram have redefined welfare delivery by embedding data at the core of governance processes.

However, this transformation is accompanied by new challenges, including centralization of power, algorithmic opacity, and the risk of exclusion. While digital systems offer unprecedented efficiency, their legitimacy depends on their ability to ensure accessibility, transparency, and accountability.

This chapter establishes that technological governance, while indispensable in contemporary administration, must be critically evaluated within constitutional and socio-economic frameworks. It sets the stage for the next chapter, which examines the **privacy and constitutional implications** of data-driven governance.

## PRIVACY, SURVEILLANCE, AND CONSTITUTIONAL IMPLICATIONS

### 4.1 Constitutional Foundations of Privacy in India

The expansion of digital governance necessitates a careful examination of its constitutional limits, particularly in relation to the right to privacy. The Supreme Court's landmark decision in *Justice K.S. Puttaswamy v. Union of India* unequivocally recognized privacy as a fundamental right intrinsic to life and personal liberty under Article 21 of the Constitution.[36]

The Court articulated privacy as encompassing multiple dimensions, including informational privacy, bodily autonomy, and decisional freedom. Importantly, it established that any infringement of privacy must satisfy a **three-fold test**:

1. **Legality** – existence of a valid law;
2. **Necessity** – legitimate state aim;
3. **Proportionality** – rational nexus and minimal intrusion.[37]

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

This doctrinal framework serves as the primary constitutional standard against which digital governance mechanisms must be evaluated.

### 4.2 Informational Privacy and Data Governance

Digital welfare platforms rely extensively on the collection and processing of personal data, including sensitive information such as health status, location, and socio-economic indicators. This raises concerns regarding **informational privacy**, which the Supreme Court in *Puttaswamy* recognized as a critical component of individual autonomy.[38]

The Digital Personal Data Protection Act, 2023 provides a statutory framework governing such data processing. It introduces key principles such as:

- **Consent-based processing**
- **Purpose limitation**
- **Data minimization**
- **Accountability of data fiduciaries**[39]

However, the Act also incorporates broad exemptions for State functions, particularly where data processing is necessary for the provision of public services or in the interest of sovereignty and public order.[40] This creates a potential tension between statutory authorization and constitutional safeguards, especially where such exemptions are interpreted expansively.

### 4.3 Surveillance Concerns in Digital Welfare Systems

The integration of digital platforms into governance has given rise to concerns regarding **surveillance and state overreach**. Applications such as Aarogya Setu, which collected location and proximity data for contact tracing, illustrate the extent to which personal data can be leveraged for public purposes.[41]

While such measures may be justified during public health emergencies, their continued use raises questions about proportionality and necessity. The absence of clear limitations on data retention and usage increases the risk of **function creep**, where data collected for one purpose is repurposed for another without adequate oversight.[42]

| | |
|---|---|
| **High Welfare Benefit** | **Moderate Surveillance (Ideal Banalnce)** |
| **Moderate Benefit** | **High Surveillance (Risk Zone)** |
| **Low Benefit** | **High Surveillance (Unconstitutional)** |

**Interpretation:**
This model demonstrates that the legitimacy of surveillance measures depends on maintaining a balance between **public benefit and privacy intrusion**, consistent with the proportionality doctrine.

### 4.4 Consent, Autonomy, and Structural Inequality

A critical issue in digital governance is the nature of **consent**. While the DPDP Act emphasizes consent as a cornerstone of data protection, the validity of consent in welfare contexts is inherently problematic.

Migrant workers often face a situation where access to essential services is contingent upon agreeing to data collection, thereby undermining the voluntariness of consent.[43] This creates what may be described as **"coercive consent,"** where individuals have no meaningful alternative but to comply.

From a constitutional perspective, such practices raise concerns regarding autonomy and dignity under Article 21. The Supreme Court has emphasized that consent must be informed, voluntary, and free from coercion, failing which it cannot serve as a legitimate basis for data processing.[44]

### 4.5 Judicial Approach to Technology and Rights

The judiciary has increasingly engaged with issues arising from technological governance. In *Anuradha Bhasin v. Union of India*, the Supreme Court recognized that access to the internet is

integral to the exercise of fundamental rights, particularly freedom of speech and expression.[45]

Similarly, in *Puttaswamy (Aadhaar)*, the Court examined the constitutionality of large-scale data collection, emphasizing the need for robust safeguards against misuse.[46] While the Aadhaar scheme was upheld, the judgment highlighted the importance of limiting data collection to what is strictly necessary.

These decisions reflect an emerging judicial framework that seeks to balance technological innovation with constitutional protections. However, the application of these principles to newer forms of digital governance remains inconsistent and evolving.

### 4.6 Comparative Perspectives on Data Protection and Surveillance

Comparative analysis reveals that jurisdictions such as the European Union have adopted more stringent approaches to data protection through instruments like the **General Data Protection Regulation (GDPR)**.[47]

Key features of such frameworks include:

- Strong consent requirements
- Independent regulatory oversight
- Strict limitations on data processing
- Rights of data subjects

In contrast, the Indian framework, while evolving, continues to provide broader exemptions for State action. This divergence highlights the need for stronger institutional safeguards to ensure that digital governance does not compromise fundamental rights. India's framework represents an **intermediate model**, balancing regulatory oversight with state flexibility, but requiring further strengthening to match global standards.

### 4.7 Proportionality and the Future of Digital Governance

The principle of proportionality remains central to evaluating the constitutionality of digital welfare systems. Any intrusion into privacy must be justified by a legitimate aim, be necessary to achieve that aim, and represent the least restrictive means available.[48]

In practice, however, the application of this principle to digital governance is complex. The scale and opacity of data-driven systems make it difficult to assess whether these conditions are satisfied. This underscores the need for:

- Transparent algorithms
- Independent oversight mechanisms
- Clear limitations on data use

The expansion of digital governance in India has fundamentally altered the relationship between the State and the individual, placing data at the center of welfare delivery. While such systems offer significant benefits in terms of efficiency and scale, they also raise profound constitutional concerns relating to privacy, autonomy, and surveillance.

The jurisprudence emerging from *Puttaswamy* and subsequent cases provides a robust framework for evaluating these concerns, emphasizing the need for legality, necessity, and proportionality. However, the practical application of these principles remains uneven, particularly in the context of large-scale digital welfare systems.

This chapter demonstrates that the challenge is not merely technological but constitutional: ensuring that the expansion of state capacity through digital means does not erode fundamental rights. It sets the stage for the final chapter, which synthesizes these findings and proposes policy directions to reconcile welfare objectives with constitutional safeguards.

## CONCLUSION AND POLICY IMPLICATIONS

### 5.1 Conclusion

The preceding chapters have examined the intersection of migrant labour, digital governance, and constitutional rights within the Indian context, particularly in the aftermath of the COVID-19 pandemic. The analysis reveals that while technological interventions have significantly enhanced the State's capacity to

manage welfare delivery, they have simultaneously introduced new forms of exclusion and constitutional complexity.

The pandemic served as a catalyst for the rapid expansion of digital governance mechanisms, transforming welfare administration into a data-centric enterprise. Platforms such as the National Migrant Information System (NMIS), Aarogya Setu, and the e-Shram portal exemplify this shift, demonstrating the State's increasing reliance on digital infrastructures to identify, monitor, and assist vulnerable populations. However, the effectiveness of these platforms is fundamentally contingent upon equitable access to digital resources—an assumption that does not hold true for large segments of India's migrant workforce.

As demonstrated earlier in Chapter 2 digital inequality remains a persistent structural barrier, manifesting in disparities in internet access, device ownership, and digital literacy. These inequalities translate directly into welfare exclusion, as individuals who are unable to engage with digital systems are effectively denied access to state benefits. The reliance on digital platforms thus risks transforming socio-economic vulnerability into digital marginalization, thereby undermining the inclusive objectives of welfare policies.

Chapter 3 further highlights the transformation of governance through the centralization of data and the emergence of algorithmic decision-making. While these developments enhance administrative efficiency, they also concentrate power within centralized systems, creating asymmetries between the State and individuals. The opacity of algorithmic processes and the absence of robust accountability mechanisms raise concerns regarding fairness and transparency in welfare delivery.

Chapter 4 situates these developments within the constitutional framework, emphasizing the centrality of privacy, autonomy, and dignity. The recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* provides a critical doctrinal foundation for evaluating digital governance practices.[49] The proportionality framework articulated by the Court requires that any intrusion into privacy be justified by legality, necessity, and minimal intrusion. However, the application of this framework to large-scale digital welfare systems remains uneven, particularly in light of statutory exemptions under the Digital Personal Data Protection Act, 2023.[50]

Taken together, the analysis reveals a fundamental paradox: **technology has become both an instrument of inclusion and a mechanism of exclusion**. While digital platforms enable the State to extend welfare benefits at an unprecedented scale, they also risk excluding those who lack access to digital resources. Similarly, while data-driven governance enhances efficiency, it raises concerns regarding surveillance and the erosion of individual autonomy.

At its core, the issue is not the use of technology per se, but the manner in which it is integrated into governance frameworks. The challenge lies in ensuring that technological innovation is aligned with constitutional values, rather than undermining them. This requires a rethinking of digital governance models to prioritize inclusivity, transparency, and accountability.

### 5.2 Policy Implications and Recommendations

The findings of this study underscore the need for a comprehensive and multi-dimensional approach to reforming digital welfare governance in India. The following policy recommendations aim to bridge the gap between technological efficiency and constitutional compliance:

#### 5.2.1 Bridging the Digital Divide

The most immediate and pressing requirement is to address the structural inequalities in digital access. Without universal access to digital infrastructure, any system of digital welfare will remain inherently exclusionary.

Policy interventions should focus on:

- Expanding rural broadband infrastructure under initiatives such as BharatNet;
- Subsidizing access to smartphones and digital devices for low-income populations;
- Promoting digital literacy programs tailored to migrant workers and informal labourers.

Bridging the digital divide is not merely a developmental objective but a **constitutional imperative**, as access to digital systems increasingly determines access to fundamental rights.[51]

#### 5.2.2 Hybrid Welfare Delivery Models

The exclusive reliance on digital platforms for welfare delivery must be reconsidered. Instead, the State should adopt **hybrid models** that combine digital systems with traditional, offline mechanisms.

Such models would ensure that individuals who are unable to access digital platforms are not excluded from welfare benefits. For instance:

- Physical registration centers for schemes such as e-Shram;
- Mobile outreach units for migrant populations;
- Integration of digital systems with local administrative bodies such as panchayats.

This approach would enhance inclusivity while retaining the efficiency benefits of digital systems.

#### 5.2.3 Strengthening Data Protection and Privacy Safeguards

While the Digital Personal Data Protection Act, 2023 represents a significant step forward, its effectiveness depends on robust implementation and enforcement.[52]

Policy measures should include:

- Narrowing the scope of state exemptions under Section 17 to prevent misuse;
- Establishing an independent and adequately empowered Data Protection Board;
- Ensuring strict compliance with principles of data minimization and purpose limitation;
- Mandating periodic audits of government data systems.

These measures are essential to ensure that the expansion of digital governance does not come at the cost of fundamental rights.

#### 5.2.4 Regulating Algorithmic Governance

The increasing use of algorithmic systems in decision-making necessitates the development of regulatory frameworks to ensure transparency and accountability.

Key interventions should include:

- Mandatory disclosure of algorithmic criteria used in welfare allocation;
- Mechanisms for individuals to challenge automated decisions;
- Independent oversight of algorithmic systems to detect bias and errors;
- Adoption of principles of **algorithmic fairness and explainability**.

Such measures would align digital governance practices with the constitutional principles of equality and non-arbitrariness under Article 14.

#### 5.2.5 Enhancing Institutional Accountability

Effective governance requires not only legal frameworks but also strong institutional mechanisms.

Reforms should focus on:

- Strengthening coordination between central and state agencies;
- Establishing grievance redressal mechanisms accessible to migrant workers;
- Ensuring transparency in data collection and usage;

- Promoting participatory governance by involving civil society and worker organizations.

Institutional accountability is critical to maintaining public trust in digital systems and ensuring their legitimacy.

### 5.2.6 Ensuring Portability and Inclusivity of Welfare Schemes

Given the mobility of migrant workers, welfare systems must be designed to ensure **portability across states and regions**.

Initiatives such as the One Nation One Ration Card (ONORC) scheme represent important steps in this direction, but further reforms are needed to integrate other welfare benefits into a portable framework.[53]

Additionally, policies must account for the specific needs of migrant workers, including language diversity, mobility patterns, and informal employment structures.

### 5.3 Concluding Reflections

The transformation of governance through digital technologies represents an inevitable and necessary evolution in the functioning of the modern State. However, this transformation must be guided by constitutional principles to ensure that it serves as a tool of empowerment rather than exclusion.

The experience of migrant workers in India illustrates the risks of uncritical reliance on technology in welfare delivery. While digital platforms have the potential to enhance efficiency and reach, they also expose structural inequalities and create new challenges for the protection of fundamental rights.

Ultimately, the success of digital governance depends on its ability to balance competing objectives: efficiency and inclusivity, innovation and accountability, welfare and privacy. Achieving this balance requires not only legal reform but also a broader commitment to **constitutional values and social justice**.

As India continues to expand its digital governance infrastructure, it must ensure that technology remains a means to an end—namely, the realization of dignity, equality, and justice for all citizens. The future of welfare governance lies not in the abandonment of technology, but in its **ethical and equitable integration** within the constitutional framework.

### REFERENCES

1. See generally Int'l Labour Org. (ILO), *ILO Monitor: COVID-19 and the World of Work* (2020).
2. See Rozin Hasin, *Prosthetics of the Indian State: The e-Shram Portal for Unorganized Workers in India* (2025) (arXiv).
3. Telecom Regulatory Authority of India (TRAI), *The Indian Telecom Services Performance Indicators* (latest reports).
4. Ministry of Labour & Employment, Govt. of India, *e-Shram Portal Overview* (2021–2025).
5. Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 1 (India) (MeitY).
6. Id. §§ 6, 10.
7. Digital Personal Data Protection Rules, 2025 (India) (Press Information Bureau).
8. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
9. Id.
10. See Government of India, Aarogya Setu App Framework & Public Discourse (2020–2022).
11. Gov't of India, *Economic Survey 2021–22* (India).
12. Periodic Labour Force Survey (PLFS), 2022–23, Ministry of Statistics & Programme Implementation (India).
13. Ministry of Home Affairs, Govt. of India, National Migrant Information System (NMIS) (2020).

14. Ministry of Labour & Employment, Govt. of India, *e-Shram Portal Dashboard* (2025).
15. Telecom Regulatory Authority of India (TRAI), *The Indian Telecom Services Performance Indicators* (2024–2025).
16. National Sample Survey Office (NSSO), *Household Social Consumption: Education & Digital Access Reports* (latest rounds).
17. See Rozin Hasin, *Prosthetics of the Indian State: The e-Shram Portal for Unorganized Workers in India* (2025).
18. Int'l Labour Org. (ILO), *India Labour Migration Report* (2022).
19. Department of Food & Public Distribution, Govt. of India, One Nation One Ration Card (ONORC) Scheme Reports (2023–2025).
20. World Bank, *Digital Development Overview Report* (2024).
21. INDIA CONST. arts. 14, 21.
22. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
23. World Bank, *World Development Report: Data for Better Lives* (2021).
24. Id.
25. Ministry of Home Affairs, Govt. of India, National Migrant Information System (NMIS) (2020).
26. Government of India, Aarogya Setu Application Framework (2020).
27. See *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
28. Ministry of Labour & Employment, Govt. of India, *e-Shram Portal Overview* (2021–2025).
29. World Bank, supra note 23.
30. Id.
31. See generally OECD, *Artificial Intelligence in Society* (2019).
32. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
33. Id. §§ 4–8.
34. Id. § 17.
35. Digital Personal Data Protection Rules, 2025 (India).
36. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
37. Id.
38. Id.
39. Digital Personal Data Protection Act, 2023, §§ 4–8 (India).
40. Id. § 17.
41. Government of India, Aarogya Setu Application Framework (2020).
42. World Bank, supra note 23.
43. See OECD, *Artificial Intelligence in Society* (2019).
44. *Puttaswamy*, (2017) 10 SCC 1 (India).
45. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
46. *K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1 (India).
47. Regulation (EU) 2016/679 (General Data Protection Regulation).
48. *Puttaswamy*, (2017) 10 SCC 1 (India).
49. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
50. Digital Personal Data Protection Act, 2023, § 17 (India).
51. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
52. Digital Personal Data Protection Act, 2023 (India).
53. Department of Food & Public Distribution, Govt. of India, One Nation One Ration Card (ONORC) Scheme Reports (2023–2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in