iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74280

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Data, Ethics, and Power: Reimagining the Social Contract in the Digital Age

Dr. Subasish Mohanty[1], Dr. Nisha Sawant[2] ,Dr. Shruti Kirti[3], Mr. Dnyandev Khadapkar[4]
[1]*Assistant Professor, Department of Commerce, Goa Multi-Faculty College*
[2]*Assistant Professor, Department of Computer Applications and IT, Goa Multi-Faculty College*
[3]*Freelance Researcher & Sr. Teacher, TGS*
[4]*Assistant Professor, Department of Computer Applications and IT, Goa Multi-Faculty College*

Abstract: ***The exponential growth of digital technologies and the pervasive use of data in governance, commerce, and everyday life have fundamentally altered the traditional foundations of the social contract. Historically, the social contract has symbolized a mutual agreement between the state and its citizens, predicated on trust, accountability, and the equitable distribution of rights and responsibilities. However, in the digital age, the dynamics of this contract are being renegotiated under the influence of three powerful forces: datafication, algorithmic decision-making, and the asymmetrical control of digital infrastructure.***
In this paper, we examine the complex relationship between data, ethics, and power in shaping the future of the social contract, with a particular emphasis on the Indian context. The unregulated extraction, commodification, and surveillance of personal data by both state and private actors raise critical ethical questions about consent, autonomy, and digital rights. Simultaneously, the growing reliance on AI and machine learning in public policy and welfare delivery introduces concerns around algorithmic bias, opacity, and exclusion. These developments often concentrate power in the hands of a few tech corporations and state bodies, exacerbating existing social inequalities and diminishing citizen agency.
India's digital transformation—epitomized by platforms like Aadhaar, Digital India, and the growing use of AI in governance—presents a dual-edged scenario. On one hand, data-driven innovations have enhanced access to services, financial inclusion, and administrative efficiency. On the other, they have amplified risks of data misuse, discrimination, and surveillance without robust legal safeguards. The absence of a comprehensive data protection law, weak enforcement mechanisms, and limited digital literacy compound these vulnerabilities.
This paper argues for the urgent need to reimagine the social contract in the digital era—one that centers ethical data practices, transparent governance, and participatory oversight. It explores the normative foundations of a new data ethics framework that prioritizes user dignity, consent, accountability, and distributive justice. It also discusses the potential of decentralized technologies, civic tech initiatives, and digital constitutionalism in redistributing power and restoring trust in digital institutions.
Keywords: Data ethics, social contract, digital governance, algorithmic power, digital rights, surveillance, India, data justice, civic tech, AI ethics.

I. INTRODUCTION

The classical theory of the social contract, as articulated by Hobbes, Locke, and Rousseau, outlined a framework where individuals consent to give up certain freedoms in exchange for state protection and social order. In the twenty-first century, this contract is being redefined under the pressures of digital technologies, massive datafication, and algorithmic governance. Data has emerged as the new resource of power, shaping relationships between the state, corporations, and citizens. While digital transformation promises efficiency, transparency, and inclusion, it simultaneously raises profound ethical concerns around privacy, surveillance, and inequality. This paper examines these challenges with a focus on India and explores how the social contract might be reimagined for the digital era.

II. LITERATURE REVIEW

The literature on data ethics and governance has expanded significantly. Shoshana Zuboff (2019) characterizes the phenomenon of *surveillance capitalism*, where corporations monetize personal data, often without meaningful consent. Lawrence Lessig (1999) argued that *code is law*, emphasizing how digital architectures can regulate behavior as effectively as traditional law. Couldry and Mejias (2019) describe *data colonialism*, warning that global technology platforms extract value from citizens in ways reminiscent of historical colonial exploitation.

Other scholars point to the broader implications of surveillance. Lyon (2018) stresses that surveillance has become embedded in everyday life, creating a *culture of surveillance*. Andrejevic (2014) notes that online economies generate forms of alienation, as individuals become objects of constant monitoring and profiling. Similarly, boyd and Crawford (2012) raise critical questions about the epistemological and ethical assumptions of "big data," particularly its claim to objectivity and comprehensiveness.

Algorithmic governance has also attracted growing scholarly attention. Mittelstadt, Allo, Taddeo, Wachter, and Floridi (2016) provide a comprehensive map of ethical concerns around algorithms, including issues of bias, accountability, and opacity. Pasquale (2015) warns of the *black box society*, where secret algorithms increasingly influence decisions in credit scoring, employment, and policing. Eubanks (2018) demonstrates the real-world consequences of algorithmic decision-making on marginalized communities, showing how high-tech tools can profile and punish the poor.

From a global governance perspective, Greenleaf (2014) traces the rapid rise of data privacy laws worldwide, while West (2019) emphasizes how data capitalism is reshaping notions of privacy and surveillance. Belli and Zingales (2017) highlight how digital platforms simultaneously regulate users while evading regulation themselves, complicating the social contract between corporations and citizens.

In the Indian context, Khera (2017) has critically evaluated Aadhaar, pointing out issues of exclusion, privacy, and weak accountability mechanisms. Narayan (2020) adds that digital identity systems can deepen social inequalities if not carefully implemented. Banerjee (2021) underscores the emerging challenges of creating a coherent data governance framework in India, while Bhattacharya and Sinha (2020) analyze the risks of algorithmic governance in the Indian welfare state. Sen (2022) further stresses the tension between innovation and accountability in regulating India's digital platforms.

Together, this growing body of literature illustrates the complex interplay of technology, ethics, and governance that underpins debates on the digital social contract. It highlights the urgent need for frameworks that not only protect individual rights but also ensure fairness, transparency, and accountability in digital ecosystems.

III. METHODOLOGY

This paper uses a qualitative and conceptual approach. Secondary sources including academic journals, policy papers, and government reports are critically analyzed. The framework for analysis focuses on three pillars: (i) datafication and commodification, (ii) algorithmic governance and its ethical dilemmas, and (iii) asymmetry of power between the state, corporations, and citizens. The Indian experience is highlighted as a case study to illustrate these dynamics.

IV. DATA, ETHICS, AND POWER IN THE DIGITAL AGE

The digital revolution has transformed data into both an economic resource and a tool of governance. Datafication—the conversion of human activities into quantifiable information—enables predictive analytics, targeted advertising, and automated decision-making. While these innovations create efficiency, they also commodify citizens' lives, reducing individuals to data points for extraction and profit (Zuboff, 2019).

Algorithmic governance raises further ethical concerns. Algorithms now make decisions in credit scoring, hiring, policing, and welfare allocation, yet they often operate opaquely, with risks of bias and discrimination (Pasquale, 2015; Eubanks, 2018). Mittelstadt, Allo, Taddeo, Wachter, and Floridi (2016) caution that the opacity of algorithmic systems undermines accountability, as citizens cannot challenge decisions that affect their lives. In practice, this creates new forms of inequality, where marginalized groups are disproportionately targeted by surveillance systems or excluded from essential welfare services.

The asymmetry of power between citizens and powerful institutions—states and corporations—creates vulnerabilities that threaten democratic values and human rights. Couldry and Mejias (2019) argue that this reflects a new form of *data colonialism*, where global platforms extract value from populations in ways that replicate historical patterns of exploitation. Lyon (2018) adds that this constant monitoring leads to a *culture of surveillance*, normalizing practices of watching and recording as part of everyday life. Andrejevic (2014) further notes that online economies foster alienation, as individuals lose control over how their personal data is used.

From an economic perspective, West (2019) observes that data capitalism has redefined privacy, making surveillance an inherent feature of digital business models. This concentration of data in the hands of a few corporations not only skews market competition but also creates political risks, as governments increasingly rely on corporate infrastructures for governance. Belli and Zingales (2017) emphasize that platforms play a dual role: they regulate users' behavior through algorithms, while simultaneously resisting regulation themselves, further skewing the balance of power.

Globally, responses to these challenges vary. The European Union's GDPR represents a rights-based approach, emphasizing individual consent and data minimization. By contrast, many developing countries, including India, are still building their legal frameworks, leaving gaps in enforcement and citizen protection (Banerjee, 2021). This regulatory unevenness allows transnational corporations to exploit weak governance structures, intensifying inequalities between the Global North and South.

Thus, data, ethics, and power in the digital age must be viewed not only as technical issues but also as fundamentally political and social concerns. The digital ecosystem simultaneously enables opportunities for innovation and efficiency while also reinforcing hierarchies of control, surveillance, and exclusion. Addressing these contradictions is central to reimagining the social contract in the twenty-first century.

V. THE INDIAN CONTEXT

India provides a unique lens to study the digital social contract. Aadhaar, the world's largest biometric identity system, has enabled direct transfers of subsidies and benefits, reducing corruption and inefficiencies. However, it has also raised concerns about data security, misuse, and the exclusion of vulnerable populations (Khera, 2017). The Digital India initiative envisions a technology-driven transformation of governance, but gaps in digital literacy and access risk deepening inequality. Moreover, until recently India lacked a comprehensive data protection law, leaving citizens without robust safeguards. The passage of the Digital Personal Data Protection Act is a step forward, yet challenges of implementation and enforcement remain significant.

VI. REIMAGINING THE SOCIAL CONTRACT

The reimagining of the social contract in the digital era requires embedding ethics and accountability in governance frameworks. Ethical data governance must ensure informed consent, equitable access, transparency in usage, and strict accountability for misuse. Beyond compliance, it should foster trust between citizens, corporations, and the state.

The idea of *digital constitutionalism* emphasizes embedding fundamental rights—such as privacy, equality, and freedom of expression—into the very design of digital infrastructures. This ensures that technologies operate within a framework of justice and fairness, rather than simply maximizing efficiency or profit.

Emerging decentralized technologies like blockchain and civic tech platforms have the potential to empower citizens by reducing dependence on centralized authorities and providing more transparent decision-making systems. In parallel, participatory oversight mechanisms, such as citizen data trusts or independent review boards, could play a vital role in rebalancing power, giving individuals greater control over how their data is collected, stored, and used.

In essence, reimagining the social contract is about aligning digital transformation with democratic values, so that technological progress enhances, rather than undermines, the dignity and rights of citizens.

VII. DISCUSSION

India stands at a crossroads. On one side, digital technologies offer opportunities for inclusive growth, efficient governance, and enhanced transparency. On the other, they carry risks of surveillance, exclusion, and exploitation. A comparative look at the European Union's GDPR shows how comprehensive regulation can protect citizen rights, while India is still grappling with gaps in institutional capacity and legal enforcement. The debate is not about rejecting technology, but about designing ethical frameworks that balance innovation with safeguards.

CONCLUSION AND RECOMMENDATIONS

The digital age demands a redefined social contract that addresses not only the traditional relationship between the state and its citizens but also the growing influence of corporations and global technology platforms. In this new landscape, data has become both a vital resource and a source of vulnerability. Therefore, the future of democratic governance and social justice will depend on how data is collected, processed, and regulated, and whose interests it ultimately serves.

For India, this means going beyond incremental reforms and adopting a holistic, rights-based approach to digital governance. While the Digital Personal Data Protection Act represents a critical step forward, the real test lies in its effective implementation. Ensuring citizen-centric safeguards requires strong institutions, empowered oversight bodies, and a culture of transparency.

Key Recommendations:

1) Strengthen Data Protection Frameworks: Move from procedural compliance to substantive protection of citizens' rights. This includes clearer definitions of consent, stronger penalties for misuse, and effective grievance redressal mechanisms.

2) Independent Oversight and Accountability: Establish autonomous data protection authorities with adequate resources and powers to monitor both state and private actors, free from political or corporate influence.

3) Algorithmic Transparency and Fairness: Mandate regular audits of high-impact algorithms in welfare delivery, policing, hiring, and financial services. Public disclosure of audit results can build trust and reduce the risks of bias and discrimination.

4) Digital Literacy and Inclusion: Expand large-scale programs to equip citizens with critical digital literacy, particularly among rural and marginalized populations. This reduces risks of exclusion and empowers individuals to exercise their rights effectively.

5) Participatory Data Governance: Encourage citizen participation through mechanisms like *data trusts* or community data boards, ensuring that people have a collective voice in how their information is used and monetized.

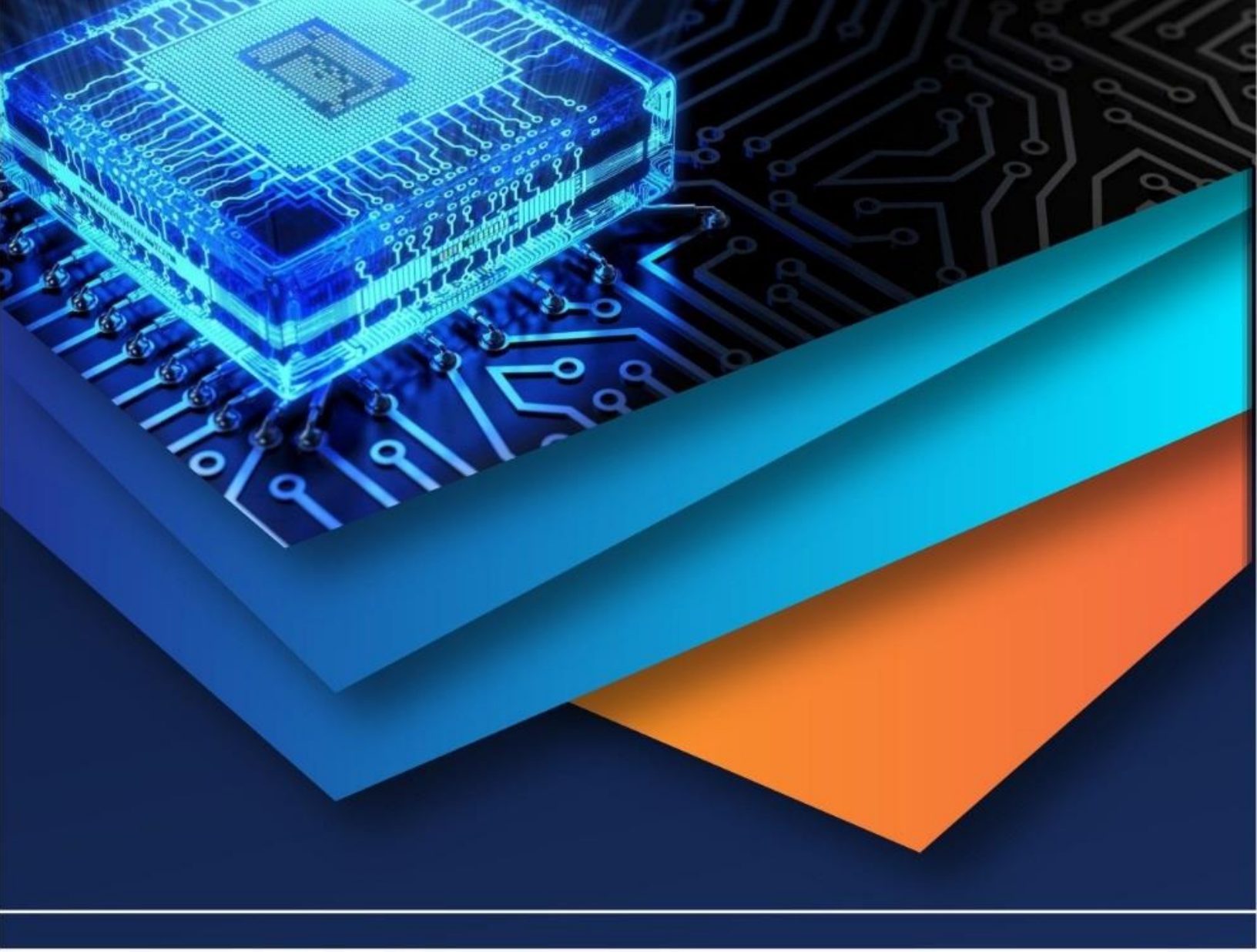
6) Platform Regulation: Create clear guidelines for digital platforms on issues such as content moderation, data portability, and cross-border data flows. This would help balance innovation with accountability.

7) Global Cooperation: As data flows transcend national borders, India should actively participate in international dialogues to shape equitable digital governance standards, preventing a new form of *data colonialism.*

In conclusion, India stands at a critical juncture. It has the opportunity to either replicate global patterns of unchecked data exploitation or emerge as a leader in developing a rights-based, inclusive model of digital governance. A renewed social contract must be forged—one that balances innovation with justice, state power with citizen agency, and data utility with human dignity. Such a contract will ensure that the promise of the digital age is realized not just for a privileged few, but for society as a whole.

REFERENCES

[1] Andrejevic, M. (2014). Surveillance and alienation in the online economy. Surveillance & Society, 12(3), 381–397. https://doi.org/10.24908/ss.v12i3.5113
[2] Arora, P. (2019). The next billion users: Digital life beyond the West. Harvard University Press.
[3] Banerjee, S. (2021). Data governance in India: Emerging frameworks and challenges. Journal of Information Policy, 11(1), 1–24. https://doi.org/10.5325/jinfopoli.11.2021.0001
[4] Belli, L., & Zingales, N. (2017). Platform regulations: How platforms are regulated and how they regulate us. Internet Policy Review, 6(4). https://doi.org/10.14763/2017.4.775
[5] Bhattacharya, D., & Sinha, A. (2020). Algorithmic governance in India: Risks and opportunities. Economic and Political Weekly, 55(47), 29–36.
[6] Bhatia, A., & Bhabha, F. (2017). India's Aadhaar scheme: The promise and perils of digital ID. Economic and Political Weekly, 52(26-27), 15-19.
[7] Boyd, d., & Crawford, K. (2012). Critical questions for big data. Information, Communication & Society, 15(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878
[8] Couldry, N., & Mejias, U. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
[9] Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
[10] Gandy, O. H. (1993). The panoptic sort: A political economy of personal information. Westview Press.
[11] Greenleaf, G. (2014). Global data privacy laws 2013: 99 countries and accelerating. Privacy Laws & Business International Report, 122, 10–13.
[12] Khera, R. (2017). Impact of Aadhaar in welfare programmes. Economic and Political Weekly, 52(50), 61-70.
[13] Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.
[14] Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.
[15] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., &Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21. https://doi.org/10.1177/2053951716679679
[16] Narayan, S. (2020). Digital identity and the Aadhaar ecosystem: Implications for inclusion and exclusion. Indian Journal of Human Development, 14(2), 239–253. https://doi.org/10.1177/0973703020959611
[17] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
[18] Sen, R. (2022). Regulating digital platforms in India: Between innovation and accountability. Journal of Digital Economy, 4(1), 12–29.
[19] West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. Business & Society, 58(1), 20–41. https://doi.org/10.1177/0007650317718185
[20] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY