



Technology and Surveillance in the Post-Pandemic Society

Jagdeep Sheoran

Research Scholar, Department of Sociology, Panjab University, Chandigarh, India.

E-mail: jagdeepsheoran01@gmail.com

Received: 08 Jul 2026; Received in revised form: 05 Aug 2026; Accepted: 08 Aug 2026; Available online: 12 Aug 2026

Abstract— The COVID-19 pandemic catalyzed a global expansion of digital surveillance systems, transforming emergency health technologies into long-term governance tools. This paper critically examines the normalization of surveillance in post-pandemic society through a sociological lens, with a particular focus on India. Drawing exclusively from secondary data, it analyzes how surveillance infrastructures – such as contact tracing apps, biometric monitoring, and AI-based public surveillance – have reconfigured state-citizen relations, reinforced social inequalities, and reshaped the meaning of citizenship in the digital age. The study engages with key sociological theories, including Foucault's governmentality, Zuboff's surveillance capitalism, and Lyon's concept of the surveillance society, to explore how technological control has been embedded into everyday life. The findings underscore that surveillance is not merely a technical phenomenon but a deeply social institution that reproduces power, marginality, and exclusion. The paper concludes with a set of policy recommendations aimed at promoting rights-based, participatory, and ethically grounded digital governance.

Keywords— Surveillance society, Digital inequality, Post-pandemic governance, Technology, Biometric surveillance, Governmentality.

I. INTRODUCTION

The COVID-19 pandemic has not only redefined the contours of public health and crisis management, but has also restructured the architecture of social control through digital means. Across the globe, including in India, surveillance technologies became central to how societies responded to the pandemic – through contact tracing apps, AI-based crowd monitoring systems, facial recognition cameras, biometric tools, and centralized data repositories. These developments, while often introduced under the pretext of necessity, raise significant sociological concerns regarding privacy, consent, inequality, and the normalization of surveillance as a mode of governance and everyday life (Lyon, 2022; Zuboff, 2019).

From a sociological standpoint, the widespread adoption of surveillance technologies must be

examined not only as a technical shift, but as a transformation in the social contract between the state and the citizen. The pandemic has accelerated what many scholars term a “digital turn” in surveillance, where bodies, movements, interactions, and even emotions are rendered into data points to be tracked and managed. This trend reflects broader structural processes of late modernity – where institutions increasingly rely on data-driven rationalities, often at the expense of human agency and democratic participation (Foucault, 1977; Giddens, 1990). The crisis has, in effect, expanded the reach of the state into the most intimate spheres of social life, and done so in ways that are unevenly distributed across class, caste, gender, and digital access lines.

In the Indian context, the deployment of digital surveillance during the pandemic has exposed and intensified pre-existing inequalities. Apps like

Aarogya Setu and platforms such as **CoWIN** assumed universal smartphone penetration and digital literacy—overlooking the structural barriers that large sections of marginalized populations face in accessing technology. Simultaneously, biometric surveillance systems like **AFRS** and **Digi Yatra** have extended state visibility into everyday spaces, often without public consent or legal oversight (Internet Freedom Foundation, 2022). These developments must be understood within the larger framework of India's technocratic policy orientation, where governance is increasingly mediated through digital infrastructures that are opaque and exclusionary.

Moreover, the discourses surrounding digital surveillance have often side-lined ethical and sociological debates in favour of narratives of security, efficiency, and modernity. This technocentric approach risks eroding the social embeddedness of rights and accountability, and instead privileges institutional convenience over citizen dignity. The normalization of such surveillance tools in the post-pandemic period indicates a reconfiguration of power—where surveillance becomes not an exception, but a permanent feature of governance, labour, mobility, and even interpersonal relations (Freedom House, 2020; Brotman, 2023).

II. CONTEXTUALIZING THE PANDEMIC AND THE RISE OF DIGITAL SURVEILLANCE

The COVID-19 pandemic triggered an unprecedented global shift not only in health infrastructure but also in the surveillance capacities of states. In the name of containing a public health crisis, countries across the world embraced a wide array of digital tools—ranging from contact tracing applications and biometric monitoring to artificial intelligence and facial recognition systems. These technologies, while introduced under the guise of emergency response, have had lasting implications on social behavior, institutional governance, and individual liberties (Lyon, 2022; Zuboff, 2019).

From the moment of crisis declaration, states sought to manage risk and uncertainty through enhanced visibility into the lives of their citizens. This shift marked a critical juncture in the evolution of state power—where technological surveillance rapidly

became a normalized, even celebrated, component of public health and security policy. However, sociological inquiry reveals that beneath this transformation lie contested terrains of control, inequality, and exclusion, which demand a critical lens beyond technocratic narratives.

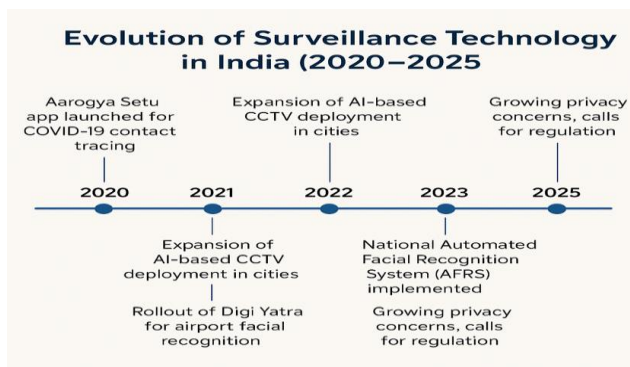
III. SURVEILLANCE AND THE RESTRUCTURING OF THE STATE-CITIZEN RELATIONSHIP

Sociologically, surveillance is not just a technical apparatus but a relational practice that alters how power operates within society. During the pandemic, the boundary between citizen and subject blurred as individuals were asked—or compelled—to submit personal data in the name of collective safety. Health became securitized, and everyday behaviors were rendered trackable and governable through digital means (Foucault, 1977; Giddens, 1990).

This shift also reconfigured the public-private divide. Digital infrastructures, often developed in collaboration with private tech firms, extended the logic of surveillance capitalism into the realm of public governance. As a result, state power increasingly operated through algorithms, databases, and mobile applications, redefining the norms of citizenship, rights, and accountability. In many cases, consent was assumed, legal safeguards were absent, and public deliberation was side-lined.

IV. DIGITAL INEQUALITIES AND THE INDIAN EXPERIENCE

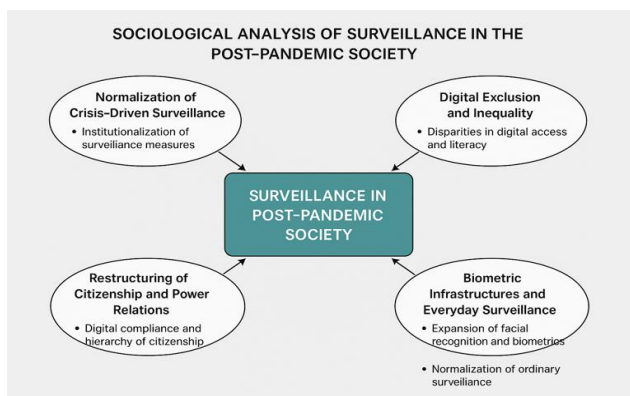
India's pandemic response presents a revealing case of how digital surveillance intersects with deeply embedded social stratifications. Tools like the **Aarogya Setu** contact tracing app and the **CoWIN** vaccine registration platform were designed under the assumption of universal digital access and literacy. However, a significant portion of India's population remains digitally marginalized—particularly among rural communities, women, Dalits, and informal workers (Internet Freedom Foundation, 2022).



Moreover, the post-pandemic period has witnessed the growth of more permanent surveillance infrastructures such as the **National Automated Facial Recognition System (AFRS)**, **Digi Yatra** for air travel, and AI-enabled CCTV monitoring in urban spaces. These technologies, while often positioned as symbols of modern governance, operate with minimal oversight and exacerbate existing inequalities in access, privacy, and representation. The convergence of biometric data collection, predictive analytics, and centralized governance without a comprehensive data protection law heightens the sociological urgency of this discourse.

V. THE SOCIOLOGICAL IMPLICATIONS OF NORMALIZED SURVEILLANCE

The normalization of digital surveillance beyond the pandemic moment reveals a deeper transformation in the moral and institutional frameworks of modern society. What began as temporary public health measures have, in many instances, evolved into permanent mechanisms of monitoring and control – raising fundamental concerns about autonomy, social trust, and digital citizenship.



Surveillance is no longer a tool of exception; it is now embedded into the routines of education, mobility, labour, and even social welfare. This has given rise to

what scholars term the “post-pandemic surveillance society,” where citizens are increasingly governed through data, and visibility itself becomes a site of power (Freedom House, 2020; Brotman, 2023). As sociologists, it is critical to interrogate who is being seen, who is invisible, and what consequences this has for social inclusion, resistance, and governance.

VI. REVIEW OF LITERATURE

The literature on technology and surveillance has witnessed significant evolution in the wake of the COVID-19 pandemic, prompting new questions about the balance between public health imperatives and democratic values. Sociological scholarship, in particular, has been instrumental in highlighting how surveillance technologies intersect with power, inequality, and state-citizen dynamics.

6.1. Surveillance, Risk, and Governmentality in the Pandemic Context

Michel Foucault’s concept of *governmentality* offers a foundational lens to understand pandemic surveillance, where the state governs not just through laws but through the management of populations and bodies. The deployment of technologies like thermal scanners, drones, and mobile tracing apps during COVID-19 reflects what Lyon (2022) describes as “pandemic surveillance” – a biopolitical response that merges health governance with real-time monitoring.

Scholars like Hu (2022) and Brotman (2023) argue that the pandemic has re-legitimized surveillance under the framework of emergency. This “state of exception” normalizes previously contentious surveillance measures, making them appear both inevitable and benign. Surveillance, once critiqued for infringing on liberties, has been repackaged as a civic duty.

6.2. Surveillance Capitalism and the Role of Private Actors

Zuboff’s (2019) concept of *surveillance capitalism* – where corporations monetize behavioral data – became acutely relevant during the pandemic. Tech firms played a pivotal role in designing contact tracing systems, cloud infrastructure, and biometric platforms. Scholars like Couldry and Mejias (2020) caution that this blurring of boundaries between state and corporate surveillance leads to what they call *data*

colonialism—a new mode of social domination through information extraction.

In India, this was evident in the lack of transparency in the development of apps like Aarogya Setu, which involved private partners but was initially shielded from public audits. The digital surveillance apparatus thus emerges not only as a tool of governance but also as a commercial ecosystem that reinforces data inequalities and reduces citizens to data subjects.

6.3. Surveillance and Structural Inequality in the Indian Context

The Indian case highlights the uneven consequences of technology-led surveillance. As Dvara Research (2020) and the Internet Freedom Foundation (2022) point out, surveillance infrastructures assume digital access and literacy, ignoring the vast exclusion of women, rural populations, Dalits, Adivasis, and informal sector workers.

George and Sureshkumar (2021) argue that in societies with socio-economic stratification, surveillance amplifies marginality. For example, those without smartphones were unable to register for vaccines via the CoWIN portal, effectively turning access to healthcare into a function of digital inclusion. Surveillance systems, rather than being neutral, are embedded in existing hierarchies and often deepen them.

6.4. Ethical and Legal Dilemmas of Post-Pandemic Surveillance

A consistent concern in the literature is the absence of adequate legal frameworks to regulate pandemic surveillance. In India, despite growing biometric

databases and AI-powered policing, there is no national data protection law—a gap that leaves millions without legal recourse in the event of misuse (Freedom House, 2020).

International organizations like the OECD (2020) and WHO (2022) have called for stronger governance mechanisms, ethical safeguards, and participatory frameworks to ensure that technological interventions respect fundamental rights. Scholars warn that surveillance systems implemented during a crisis are rarely dismantled post-crisis, leading to long-term erosion of privacy and autonomy.

6.5. Emerging Frameworks for Rights-Based Digital Governance

Recent sociological scholarship has begun to push back against deterministic narratives of surveillance, proposing alternative frameworks rooted in accountability, transparency, and co-governance. Lyon (2022) advocates for a “surveillance ethics” approach, wherein technology must be evaluated not only by its efficiency but also by its social and moral costs.

Buhmann (2023) emphasizes the need for community-centered digital governance models that incorporate local knowledge, particularly in the Global South. Similarly, the SSRC (2021) highlights that any post-pandemic surveillance policy must be inclusive, rights-aware, and adaptable to plural socio-political contexts. These contributions form a critical foundation for reimagining surveillance not as a fixed system but as a negotiable space of power and resistance.

Table: Research Gaps Identified from Literature Review

Area of Focus	Literature Insights	Identified Gap
Emergency Surveillance Technologies	Most studies focus on contact tracing and pandemic-era apps like Aarogya Setu and CoWIN.	Lack of analysis on how these technologies are institutionalized post-pandemic.
Geographical Context	Global North dominates the discourse, particularly U.S. and Europe.	Limited sociological analysis of surveillance in Global South, especially India.
Inequality and Exclusion	Digital exclusion is mentioned in passing.	Insufficient exploration of caste, class, gender, and rural-urban digital divides in India.
Citizen Experience and Agency	Focus is mainly on legal or technological dimensions of surveillance.	Absence of sociological studies on lived experiences of surveillance among vulnerable groups.

Governance and Accountability	Emerging frameworks for ethical AI and digital rights are being discussed.	Need for interdisciplinary, participatory, rights-based governance models tailored to local contexts.
-------------------------------	--	---

VII. RESEARCH GAP

Despite the growing body of literature on digital surveillance during the COVID-19 pandemic, several critical gaps persist in sociological scholarship—especially when examining long-term impacts and contextual inequalities in the Global South.

Firstly, most existing studies have concentrated on the *emergency phase* of surveillance, focusing on immediate pandemic responses such as contact tracing apps and quarantine monitoring. There is limited inquiry into the **post-pandemic institutionalization** of these technologies—how temporary measures are being absorbed into the fabric of routine governance, policing, public health, and mobility systems, often without democratic oversight.

Secondly, while surveillance capitalism and state surveillance have been analyzed at length in Western contexts (Zuboff, 2019; Lyon, 2022), there is a noticeable **geographical bias** in literature, with relatively less attention to how these systems operate in countries like India. In particular, there is a lack of detailed sociological work exploring how surveillance technologies interact with **local social hierarchies**—including caste, class, gender, and rural-urban divides. The Indian experience with tools like *Aarogya Setu*, *AFRS*, and *Digi Yatra* underscores how surveillance is not just technological but deeply embedded in socio-political power structures.

Thirdly, existing legal and policy analyses often lack a **sociological understanding of lived experiences**—how individuals perceive, negotiate, and resist surveillance in their everyday lives. Questions around consent, autonomy, fear, and digital exclusion remain under-theorized, particularly in relation to vulnerable communities who are often the most surveilled but the least protected.

Finally, while there are emerging calls for rights-based digital governance (OECD, 2020; WHO, 2022), the **absence of interdisciplinary, bottom-up frameworks**—that bring together public health, sociology, ethics, and digital rights—leaves a gap in

crafting policies that are both technologically sound and socially just.

This research seeks to address these gaps by offering a critical, context-sensitive sociological analysis of how pandemic-era surveillance technologies are shaping post-pandemic society in India. It aims to reframe surveillance not merely as a technical tool, but as a **social institution** that both reflects and reinforces existing patterns of inequality, exclusion, and control.

VIII. RATIONALE OF THE STUDY

The COVID-19 pandemic triggered an unprecedented expansion of digital surveillance technologies, originally framed as emergency public health tools. However, many of these technologies—such as contact tracing apps, biometric systems, and AI-enabled monitoring—have now become embedded in routine governance, fundamentally reshaping state-citizen relations. This shift raises urgent sociological concerns about autonomy, consent, inequality, and the normalization of control.

In India, platforms like *Aarogya Setu*, *CoWIN*, and facial recognition systems were deployed without sufficient legal safeguards or democratic oversight. Their use highlighted deep digital divides and structural exclusions, particularly affecting marginalized communities who often lacked access, representation, or protection. Surveillance in this context is not merely about data collection—it becomes a mechanism of invisibilization and differential governance.

This study, rooted in sociological inquiry, aims to critically examine how surveillance infrastructures have transitioned from temporary crisis tools to permanent instruments of power. Unlike purely legal or technical approaches, it interrogates the social implications of surveillance—how it reinforces hierarchies, redefines citizenship, and alters the nature of public life.

India’s experience remains underrepresented in global surveillance discourse. This research addresses that gap by drawing on secondary data and theory to

offer a context-sensitive analysis of post-pandemic surveillance. It calls for moving beyond the binary of “security versus privacy” to foreground questions of justice, accountability, and digital rights – particularly in the Global South.

By reclaiming a sociological perspective, this study contributes to ongoing debates on ethical, inclusive, and rights-based digital governance in the aftermath of the crisis.

IX. ANALYSIS AND DISCUSSION

9.1. The Normalization of Crisis-Driven Surveillance

One of the most striking features of the COVID-19 pandemic was the rapid normalization of digital surveillance in everyday life. Measures initially introduced as exceptional – such as thermal scanning, geolocation tracking, and mandatory health apps – quickly became embedded into routine governance. This shift reflects what David Lyon (2022) refers to as the rise of the “surveillance society,” where institutions increasingly depend on datafied visibility to exert control and manage uncertainty.

In India, the **Aarogya Setu** app and the **CoWIN** portal were deployed as core technologies for public health monitoring. However, these platforms lacked transparent privacy safeguards, and users were not always informed about how their data was being stored or shared. The socio-legal discourse surrounding these platforms reveals a blurring of boundaries between public health and state control, with little room for consent or dissent. The Indian state’s reliance on digital solutions has thus contributed to a governance paradigm that equates visibility with security and compliance.

9.2. Surveillance and Digital Exclusion

The deployment of surveillance technologies during the pandemic operated on the assumption of universal access to smartphones, digital literacy, and network connectivity – assumptions that do not hold in the Indian socio-economic context. Studies by the Internet Freedom Foundation (2022) and Dvara Research (2020) show that rural populations, women, Dalits, Adivasis, and informal workers were disproportionately excluded from these systems, either due to lack of access or fear of state scrutiny.

For instance, vaccine registration through the **CoWIN** portal became a barrier for many who lacked smartphones or the ability to navigate online forms. In this context, digital surveillance acted as a gatekeeper, further marginalizing already vulnerable populations from essential public services. The digital divide, therefore, is not merely technological but deeply sociological – rooted in intersecting systems of inequality and exclusion.

9.3. Biometric Infrastructures and Everyday Surveillance

Beyond pandemic-specific tools, India’s post-COVID surveillance landscape has expanded to include biometric-based systems such as the **Automated Facial Recognition System (AFRS)**, **Digi Yatra**, and AI-enabled policing in smart cities. These infrastructures mark a shift toward what could be called **everyday surveillance** – where citizens are monitored not only in moments of crisis but in routine activities such as travel, shopping, and accessing public spaces.

These systems function without comprehensive data protection legislation and often bypass institutional checks and balances. Their adoption reflects a growing technocratic culture within governance, where efficiency and innovation are prioritized over transparency and rights. Sociologically, this signals a transformation in how the state relates to its citizens – not as autonomous subjects, but as data profiles to be sorted, scored, and monitored.

9.4. Reconfiguring Citizenship and State-Society Relations

The expansion of surveillance has redefined the notion of citizenship in post-pandemic India. Citizens are increasingly expected to perform **digital compliance** – such as scanning QR codes, sharing biometric data, or downloading state-mandated apps – as part of accessing public services or moving through urban infrastructure. This expectation creates a hierarchy of citizenship based on digital access and technological conformity.

Foucault’s concept of **governmentality** is useful here, as it reveals how power is exercised not through coercion alone, but through practices that render individuals governable. Surveillance technologies, by demanding continuous self-monitoring and digital participation, produce a new kind of subjectivity –

one that is visible, traceable, and evaluable by the state.

9.5. Counter-Narratives and Civil Society Resistance

Amid this expansion of surveillance, civil society organizations, legal scholars, and technology ethicists have pushed back against the erosion of privacy and rights. Institutions such as the Internet Freedom Foundation and the Centre for Internet and Society have highlighted the legal vacuum around data protection and the need for democratic accountability. International bodies like the **OECD** and **WHO** have similarly emphasized the importance of rights-based digital governance frameworks.

While these counter-narratives remain fragmented, they offer an important discursive space to challenge the inevitability of surveillance. They also underline the need for inclusive, participatory technology policies that foreground consent, justice, and dignity—particularly in postcolonial contexts like India.

X. SOCIOLOGICAL IMPLICATIONS: SURVEILLANCE AS A SOCIAL INSTITUTION

The cumulative effect of pandemic-era surveillance is the emergence of surveillance as a **social institution**—one that governs behavior, reinforces hierarchies, and reshapes the architecture of public life. Surveillance is no longer confined to authoritarian regimes or exceptional circumstances; it is embedded into welfare delivery, urban planning, law enforcement, and mobility.

From a sociological lens, this shift demands critical attention to the **power-knowledge nexus**, the production of compliant citizens, and the reproduction of inequality through technological means. As surveillance becomes more data-driven and less visible, the challenge lies not only in regulating these systems, but also in **repoliticizing the discourse** around technology, rights, and resistance.

XI. CONCLUSION

The COVID-19 pandemic did more than disrupt healthcare systems and economies—it recalibrated the architecture of surveillance and social control across the globe. As this study has shown, surveillance

technologies introduced as emergency tools have gradually evolved into permanent fixtures of governance, normalizing a culture of continuous monitoring under the rhetoric of safety, efficiency, and digital modernization.

From a sociological lens, this normalization of surveillance cannot be understood in isolation from the broader dynamics of power, inequality, and institutional design. The Indian experience reveals how technological infrastructures—such as Aarogya Setu, CoWIN, AFRS, and Digi Yatra—were not merely tools for pandemic management, but instruments that deepened pre-existing digital and social divides. Access to technology, legal safeguards, and public accountability remained uneven, thereby producing a stratified surveillance regime where marginalized communities bore the brunt of exclusion, invisibility, and overregulation.

Moreover, the expansion of biometric surveillance and AI-enabled monitoring has significantly restructured the state-citizen relationship. The emergence of “digital compliance” as a condition for accessing basic services reflects a shift toward a governance model that privileges visibility, traceability, and behavioral control—often at the cost of autonomy and consent. Sociological theories of governmentality, surveillance capitalism, and disciplinary power help unpack how these technologies shape everyday life, create hierarchies of citizenship, and transform governance into a data-driven enterprise.

This research reaffirms the importance of critically examining surveillance as a social institution—one that reflects and reinforces structural inequalities while masquerading as neutral and progressive. It also highlights the need for a paradigm shift in digital governance, one that centers not only technological capability but also ethical responsibility, participatory policymaking, and inclusive justice.

As societies transition out of the pandemic, the challenge ahead lies not in whether surveillance will persist—but in how it will be governed, resisted, and reimagined. For sociology, this is not only an analytical task but a moral imperative: to ensure that the post-pandemic digital order is not merely efficient, but also equitable, democratic, and humane.

XII. POLICY RECOMMENDATIONS

- **Enact a Comprehensive Data Protection Law:** India urgently requires a robust data protection framework that clearly defines principles of consent, purpose limitation, data minimization, and accountability. Such legislation must not only regulate private entities but also place clear restrictions on state surveillance. The absence of legal safeguards currently allows biometric and AI-based technologies to operate with little transparency, heightening the risk of abuse.
- **Mandate Transparency and Public Oversight in Surveillance Projects:** All surveillance-related initiatives—especially those involving facial recognition, biometric tracking, and AI-driven monitoring—should be subject to independent audits, public impact assessments, and parliamentary oversight. Civil society actors, technologists, and ethicists must be included in governance processes to ensure multi-stakeholder accountability.
- **Ensure Equitable Digital Access Before Implementing Tech-Based Governance Tools:** Surveillance technologies that assume universal digital literacy and smartphone access deepen social exclusion. Any public health or welfare initiative leveraging digital platforms must be supplemented with offline, inclusive alternatives—particularly for rural populations, women, Scheduled Castes and Tribes, and informal sector workers.
- **Institutionalize Ethical Surveillance Guidelines:** The government should adopt a formal surveillance ethics charter guided by sociological and human rights principles. This should include a moratorium on predictive policing and indiscriminate facial recognition in public spaces until rigorous ethical reviews are conducted.
- **Create an Independent Surveillance Regulator:** A dedicated regulatory body—-independent of executive control—should be established to monitor surveillance practices, address grievances, and enforce compliance with rights-based digital governance. This body should be empowered to halt or revoke programs that are deemed harmful or discriminatory.

- **Invest in Digital Literacy and Rights Education:** Awareness about digital rights, data privacy, and surveillance implications remains low in India. Public campaigns, school curricula, and community programs must be developed to empower citizens—especially vulnerable groups—to understand and assert their digital rights.
- **Promote Open, Public Deliberation on the Future of Surveillance:** The trajectory of surveillance technology should not be shaped solely by technocrats or security experts. Transparent public consultations and democratic debates must guide decisions about what kinds of technologies are adopted, for what purpose, and under what conditions.

These recommendations are grounded in the belief that surveillance need not be synonymous with authoritarianism or exclusion. With democratic will, institutional safeguards, and inclusive dialogue, it is possible to reimagine a digital future that is both technologically capable and socially just.

REFERENCES

- [1] Brotman, S. N. (2020). *Privacy's perfect storm: Digital policy for post-pandemic times*. Brookings Institution Press.
- [2] Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- [3] Dvara Research. (2020). *COVID-19 impact on daily life (CIDL) survey*. <https://dvararesearch.com/wp-content/uploads/2020/06/COVID-19-Impact-on-Daily-Life-CIDL-Survey.pdf>
- [4] European Center for Not-for-Profit Law (ECNL). (2022). *Under surveillance: (Mis)use of technologies in emergency responses*. <https://ecnl.org/sites/default/files/2022-12/Full%20Report%20Under%20Surveillance%20-%20%28Mis%29use%20of%20Technologies%20in%20Emergency%20Responses.pdf>
- [5] Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books.
- [6] Freedom House. (2020). *Freedom on the net 2020: The pandemic's digital shadow*. <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>
- [7] Giddens, A. (1990). *The consequences of modernity*. Stanford University Press.

- [8] Hu, M. (2022). *Pandemic surveillance: Privacy, security, and data ethics*. Edward Elgar Publishing.
- [9] Internet Freedom Foundation. (2022). *Facial recognition in India: A threat to privacy and dignity*. <https://internetfreedom.in/facial-recognition-in-india-part>.
- [10] Lyon, D. (2022). *Pandemic surveillance*. Polity Press.
- [11] Organisation for Economic Co-operation and Development (OECD). (2020). *Dealing with digital security risk during the coronavirus (COVID-19) crisis*. <https://www.oecd.org/digital/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis.pdf>.
- [12] Satpute, A. D., Rai, P., & Onkar, P. (2024). Driving sustainable mobility: A study of electric vehicle adoption in rural India. In *Proceedings of the Design Society*, 4, 1427–1436. <https://doi.org/10.1017/pds.2024.145>.
- [13] Social Science Research Council (SSRC). (2021). *Surveillance and the 'new normal' of COVID-19: Public health, data, and justice*. <https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report>.
- [14] World Health Organization (WHO). (2022). *The WHO Hub for Pandemic and Epidemic Intelligence: Donor report 2022*. <https://pandemichub.who.int/docs/librariesprovider/2/default-document-library/pandemic-hub-2022-donor-report-2022.pdf>.
- [15] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.