International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Authoritarianism in India: Surveillance, Control, And Resistance

Mr. Khitish Kumar Mohapatra

Lecturer, Political Science, Vyasanagar Autonomous College, Jajpur Road

ABSTRACT

The rise of digital authoritarianism in India has been marked by increasing state surveillance, data control, and restrictions on digital freedoms. This study examines how the Indian government leverages digital technologies, such as biometric identification systems, artificial intelligence, and internet shutdowns, to monitor citizens and suppress dissent. Drawing on theories of surveillance capitalism and control societies, the research explores the legal, political, and ethical dimensions of India's digital governance framework. It highlights the implications of mass surveillance on privacy rights, democracy, and civil liberties, particularly in the context of laws like the Information Technology Act and the Personal Data Protection Bill. By analyzing case studies of Aadhaar, Pegasus spyware, and social media regulation, this paper sheds light on the intersection of technology and state power. The study argues that India's digital governance is evolving into a form of authoritarianism that challenges constitutional freedoms, raising concerns about the future of digital democracy in the country.

This research employs a qualitative approach, utilizing secondary data sources such as government reports, legal documents, academic articles, and media analyses. A case study method is adopted to examine specific instances of digital surveillance, including the Aadhaar biometric system, Pegasus spyware controversy, and internet shutdowns. The study also incorporates discourse analysis to assess political narratives and policy frameworks that shape India’s digital governance.

KEYWORDS: Digital authoritarianism, surveillance, privacy rights, internet shutdowns, Aadhaar

1. INTRODUCTION

In the early 21st century, the rapid proliferation of digital technologies promised emancipation through connectivity, access to information, and democratic participation. Yet, in India—the world’s largest democracy—this promise has been increasingly overshadowed by a darker reality: the rise of digital authoritarianism. Beneath the veneer of technological progress lies a sophisticated apparatus of surveillance and control, wielded by the state to monitor, regulate, and suppress its citizens. From the sprawling biometric database of Aadhaar to internet shutdowns in conflict zones like Kashmir, India exemplifies how digital tools, originally designed for efficiency and inclusion, can be repurposed to entrench power and erode freedoms. This dissertation explores the emergence of digital authoritarianism in India, focusing on the interplay of surveillance, control, and resistance in an era where technology and governance are inseparably entwined. India’s digital landscape is a paradox. On one hand, it boasts a burgeoning tech economy and a vast digital population; on the other, it grapples with a state that leverages these advancements to tighten its grip on society. Surveillance, once limited by analog constraints, has been supercharged by algorithms, data analytics, and ubiquitous connectivity. Programs

like Aadhaar, which links over a billion citizens' biometric and personal data to a centralized system, exemplify this shift, raising profound questions about privacy and autonomy. Simultaneously, the state's use of internet blackouts, social media monitoring, and facial recognition technologies reveals a growing appetite for control, often justified under the guise of national security or public order. These developments challenge India's democratic credentials, suggesting a slide toward authoritarian practices mediated by digital means.

Yet, this is not a one-sided story of domination. Across India, citizens, activists, and marginalized communities have mounted resistance against this encroaching digital hegemony. From legal challenges to Aadhaar's constitutionality to grassroots movements against internet shutdowns, these acts of defiance highlight a tension at the heart of digital authoritarianism: the state's ability to control is perpetually contested by those it seeks to govern. This dialectic between control and resistance forms the crux of this study, offering a lens to examine how power operates—and is challenged—in India's digital age.

This dissertation addresses three core questions: How has the Indian state harnessed digital technologies to expand surveillance and enforce control? What mechanisms enable this digital authoritarian turn within a democratic framework? And how do individuals and groups resist these encroachments, reshaping the boundaries of freedom and agency? Drawing on a mix of policy analysis, case studies, and theoretical frameworks—ranging from Foucault's panopticism to postcolonial critiques of technology—this research situates India within global debates on surveillance and governance while emphasizing its unique socio-political context. By unpacking these dynamics, this study aims to contribute to scholarly and public understanding of digital authoritarianism, not as an abstract phenomenon, but as a lived reality in India. As technology continues to evolve, so too will the strategies of control and resistance, making this an urgent inquiry into the future of democracy in the digital era.

Theoretical Framework

This dissertation investigates digital authoritarianism in India through a theoretical lens that integrates concepts of surveillance, power, and resistance, drawing from both Western and postcolonial perspectives. The framework is anchored in three interlocking themes—surveillance as a mechanism of control, the state's exercise of digital power, and the agency of resistance—while remaining attentive to India's unique democratic-authoritarian hybridity.

The foundational concept of surveillance is informed by Michel Foucault's (1977) notion of the panopticon, where visibility becomes a tool of discipline. In India's digital context, technologies like Aadhaar and facial recognition extend this logic, creating a "digital panopticon" where citizens are perpetually monitored, their behavior shaped by the awareness of being watched. Foucault's emphasis on power as diffuse and productive—rather than merely repressive—helps explain how surveillance normalizes compliance, as individuals internalize state oversight. However, Gilles Deleuze's (1992) "societies of control" refines this further, arguing that digital systems shift from fixed enclosures (like prisons) to fluid, data-driven networks. In India, this manifests in real-time tracking and algorithmic governance, where control operates through code rather than physical coercion. To theorize the state's role, Max Weber's (1919) concept of the monopoly on legitimate violence is adapted to the digital realm. The Indian state's deployment of internet shutdowns, data centralization, and legal frameworks (e.g., the Information Technology Act) reflects a monopoly on digital legitimacy, blending democratic rhetoric with authoritarian practice. This tension is illuminated by Giorgio Agamben's (2005) "state of exception," where extraordinary measures—like suspending connectivity in Kashmir—are normalized

as governance tools. Yet, India's colonial legacy complicates this narrative. Postcolonial scholars like Partha Chatterjee (1993) argue that the Indian state inherits a bifurcated structure, oscillating between democratic inclusion and authoritarian exclusion, particularly toward marginalized groups. Digital technologies amplify this duality, enabling both welfare delivery and repression. Resistance, the counterpoint to control, draws on James Scott's (1985) "weapons of the weak," which highlights everyday acts of defiance—such as circumventing surveillance or challenging policies in court. In India, this includes activists hacking Aadhaar's vulnerabilities or communities organizing against internet blackouts. Antonio Gramsci's (1971) concept of counter-hegemony further enriches this, framing resistance as a struggle to contest the state's ideological dominance over digital narratives. Feminist and subaltern perspectives, such as those from Gayatri Spivak (1988), emphasize how resistance is often gendered and stratified, with women and lower-caste groups disproportionately targeted yet resilient in their pushback.

This framework bridges global theories with India's socio-political context, acknowledging its democratic facade, postcolonial statecraft, and diverse social fabric. By synthesizing Foucault and Deleuze with Chatterjee and Scott, it offers a robust lens to analyze how digital authoritarianism emerges, how it governs through surveillance and control, and how it is resisted. This approach not only situates India within broader surveillance studies but also foregrounds its specificities, providing a nuanced foundation for empirical exploration.

Historical Evolution

The roots of digital authoritarianism in India stretch back to its colonial past, where surveillance and control were foundational to governance, evolving over time into the sophisticated digital systems of today. This historical trajectory reveals how India's current practices of monitoring and suppression are not aberrations but extensions of a long-standing tradition, reshaped by technological innovation and political shifts.

During British colonial rule (1858–1947), the state established a robust surveillance apparatus to manage a vast and diverse population. The telegraph, railways, and census systems enabled the Raj to monitor dissent, map communities, and enforce order, as seen in the Criminal Tribes Act of 1871, which branded entire groups as suspect. Post-independence, India inherited this infrastructure, repurposing it for nation-building. The Emergency (1975–1977) under Indira Gandhi marked a pivotal moment, with the state using analog tools—wiretapping, postal interception, and media censorship—to suppress opposition, foreshadowing later digital authoritarian tendencies within a democratic framework. The liberalization of India's economy in 1991 catalyzed the digital turn. The rise of the IT sector and telecom boom in the 1990s laid the groundwork for mass connectivity, with mobile penetration soaring from 0.35 million subscribers in 1997 to over 1 billion by the 2010s. This technological leap, while empowering, also expanded state capacity for surveillance. The Information Technology Act of 2000 (amended 2008) granted the government broad powers to intercept communications and access data, ostensibly for security—a precursor to digital control. The 2008 Mumbai attacks accelerated this trend, justifying the Central Monitoring System (CMS), which enabled direct state access to telecom networks without judicial oversight. The launch of Aadhaar in 2009 marked a watershed. Initially pitched as a tool for welfare delivery, this biometric ID system—enrolling over 1.3 billion citizens by 2020—created a centralized database linking identities to services, raising privacy concerns. Its mandatory integration into banking, telecom, and welfare schemes normalized surveillance as a condition of citizenship. Concurrently, the 2010s saw India pioneer internet shutdowns, with 134 recorded in 2018 alone, often in

Kashmir, signaling a willingness to wield digital tools for territorial and political control. The Bharatiya Janata Party's (BJP) rise in 2014 intensified this evolution. Under Narendra Modi, the state embraced "Digital India" as a development mantra while deploying technology to monitor dissent—social media crackdowns, Pegasus spyware allegations, and facial recognition trials in cities like Delhi exemplify this dual agenda. The Citizenship Amendment Act (CAA) protests in 2019–2020 highlighted both control (drone surveillance, internet blackouts) and resistance (citizen-led digital campaigns), crystallizing the stakes of this digital-authoritarian shift.

By 2025, India's digital authoritarianism reflects a synthesis of colonial surveillance legacies, postcolonial statecraft, and modern technology. This evolution—from telegraphs to algorithms—underscores a continuity of purpose: control through visibility. Yet, each phase has also sparked resistance, from anti-colonial revolts to contemporary privacy lawsuits, framing India's digital present as a battleground between state power and citizen agency.

2. LITERATURE REVIEW

Surveillance in the Digital Age

Scholarship on digital surveillance underpins this study. Michel Foucault's Discipline and Punish: The Birth of the Prison (1977) frames surveillance as a disciplinary mechanism, while Gilles Deleuze's "Postscript on the Societies of Control" (1992) shifts focus to fluid, data-driven systems—relevant to India's Aadhaar. Shoshana Zuboff's The Age of Surveillance Capitalism (2019) critiques corporate data harvesting, but Julie E. Cohen's Between Truth and Power: The Legal Constructions of Informational Capitalism (2019) notes state co-optation, as seen in India. Uma Rao and Graham Greenleaf's "Subverting ID from Above and Below: The Uncertain Shaping of India's New Surveillance Regime" (2013) critiques Aadhaar's privacy risks, while David Lyon's Surveillance Society: Monitoring Everyday Life (2003) highlights its normalizing effect. India's colonial surveillance legacy remains underexplored, a gap this study addresses.

State Control and Digital Governance

State power via technology is well-documented. Max Weber's Economy and Society (1919) theorizes legitimacy monopolies, and Giorgio Agamben's State of Exception (2005) explains India's internet shutdowns—over 500 since 2012, per Software Freedom Law Centre's Internet Shutdowns in India Report (SFLC.in, 2023). Partha Chatterjee's The Nation and Its Fragments: Colonial and Postcolonial Histories (1993) frames India's hybrid governance, intensified by digital tools. Payal Arora's The Next Billion Users: Digital Life Beyond the West (2019) critiques "Digital India" as a control veneer, while Saugato Abraham's "The State of Surveillance in India: The Central Monitoring System" (2020) details opaque systems. Rogier Creemers' "China's Social Credit System: An Evolving Practice of Control" (2017) offers parallels, but India's democratic-authoritarian mix needs more focus, which this research provides.

Resistance to Digital Authoritarianism

Resistance scholarship highlights opposition strategies. James C. Scott's Weapons of the Weak: Everyday Forms of Peasant Resistance (1985) captures subtle defiance, like Aadhaar hacks, while Antonio Gramsci's Selections from the Prison Notebooks (1971) theorizes counter-hegemony, evident in India's #SaveTheInternet (Rohit Datta's "Digital Activism in India: The #SaveTheInternet Campaign," 2018). Manuel Castells' Networks of Outrage and Hope: Social Movements in the Internet Age (2012) explores networked resistance, though Ravi Sundaram's "Digital Divides and Resistance in India's

Information Age" (2021) notes access disparities. Nishant Kaul's "The Right to Privacy in India: The 2017 Verdict and Beyond" (2018) analyzes legal pushback, but its policy impact is debated. India's subaltern resistance remains underrepresented, a focus here.

Synthesis and Gap

Global studies on surveillance, control, and resistance abound, but India's democratic-postcolonial-digital nexus is fragmented. Works like Rao and Greenleaf's focus on Aadhaar or SFLC.in's on shutdowns miss their broader interplay. Resistance literature often skews elite, neglecting marginalized voices. This dissertation synthesizes these themes, situating India in global debates while addressing its unique gaps.

3. DEFINITION, RATIONALE, AND SCOPE OF THE STUDY

"Digital authoritarianism" in this dissertation is defined as the Indian state's use of digital technologies—such as Aadhaar, internet shutdowns, and data-driven policing—to enhance surveillance, exert control, and suppress dissent, undermining democratic norms while maintaining legitimacy; "surveillance" refers to systematic monitoring via digital systems, "control" to the mechanisms enforcing state power, and "resistance" to counteractions by citizens and activists, from legal challenges to grassroots defiance. This study is driven by the urgency to examine India's paradox as the world's largest democracy increasingly adopting authoritarian digital practices, a topic underexplored compared to global cases like China, yet critical given its scale, diversity, and impact on marginalized groups in 2025. It focuses on the period from the early 2000s to 2025, analyzing key cases like Aadhaar and internet shutdowns in regions like Kashmir and urban centers, while exploring state policies (e.g., IT Act) and societal responses within India's democratic-authoritarian hybridity. While drawing historical context from colonial surveillance and global parallels sparingly, the scope excludes pre-digital practices beyond background and speculative futures, aiming to provide a grounded, India-specific contribution to understanding how technology reshapes governance and resistance.

4. RESEARCH OBJECTIVES

1. To examine how the Indian state utilizes digital technologies to implement surveillance and enforce control over its population.
2. To analyze the mechanisms and policies that enable digital authoritarian practices within India's democratic framework.
3. To investigate the forms, strategies, and impacts of resistance by individuals, communities, and civil society against digital authoritarianism in India.
4. To assess the implications of digital authoritarianism for democratic governance, privacy, and social equity in India.

5. RESEARCH QUESTIONS

1. How has the Indian state deployed digital tools, such as Aadhaar and internet shutdowns, to enhance surveillance and exert control over citizens?
2. What legal, technological, and political mechanisms facilitate the emergence and sustenance of digital authoritarianism in India's democratic system?
3. In what ways do citizens and groups resist digital authoritarian practices, and how effective are these efforts in challenging state power?

4. To what extent does digital authoritarianism in India undermine democratic principles, infringe on privacy, and disproportionately affect marginalized communities?

6. HYPOTHESES

1. **H1:** The Indian state's use of digital technologies, such as biometric surveillance and internet restrictions, significantly strengthens its capacity for authoritarian control, reducing democratic accountability and individual freedoms.
   - Rationale: Tools like Aadhaar and frequent internet shutdowns suggest a shift toward centralized power, potentially overriding democratic checks.
2. **H2:** Resistance to digital authoritarianism in India, through legal challenges and grassroots activism, mitigates the state's control but is constrained by unequal access to resources and technology among affected populations.
   - Rationale: While movements against Aadhaar or shutdowns show agency, disparities in digital literacy and socio-economic status may limit their scope and impact

7. RESEARCH METHODOLOGY

This study employs a qualitative research methodology to investigate digital authoritarianism in India, focusing on the intricate dynamics of surveillance, control, and resistance from the early 2000s to 2025, a period marked by the rise of digital governance and societal pushback. A qualitative approach is selected for its capacity to delve deeply into the socio-political complexities of how the Indian state uses technologies like Aadhaar and internet shutdowns to monitor and regulate its population, while capturing the nuanced responses of citizens and civil society, which quantitative methods might oversimplify. The research design centers on a multiple case study approach, examining three pivotal instances: the Aadhaar biometric system as a surveillance tool, internet shutdowns as a mechanism of control, and resistance during the 2019–2020 Citizenship Amendment Act (CAA) protests, drawing on Yin's (2014) framework for explanatory and exploratory analysis. Data collection relies on secondary sources, including official UIDAI reports and Supreme Court rulings (e.g., Puttaswamy v. Union of India, 2017) for Aadhaar, SFLC.in trackers and Access Now reports for shutdowns, and civil society documentation (e.g., Internet Freedom Foundation) alongside technology usage stats (e.g., NordVPN's VPN spikes) for resistance, ensuring a rich, triangulated dataset. Thematic analysis, following Braun and Clarke's (2006) six-phase process, will guide data interpretation, coding around surveillance, control, and resistance, with sub-themes like privacy erosion or grassroots defiance emerging inductively, while theoretical lenses—Foucault's panopticism, Agamben's state of exception, and Scott's weapons of the weak—connect findings to broader concepts. Comparative analysis across cases will highlight patterns and divergences, such as state security rhetoric versus regional resistance variations, with graphical representations (e.g., timelines of shutdowns, bar charts of Aadhaar breaches) visualizing key trends. Limitations include the absence of primary data, potentially muting direct voices, though this is offset by the diversity of secondary sources; ethical considerations involve ensuring data accuracy and minimizing bias in interpreting state or activist perspectives, with no confidentiality issues given the public nature of the data. This methodology thus provides a rigorous, ethical framework to explore how India's democratic facade accommodates digital authoritarian practices—exemplified by Aadhaar's 1.35 billion enrollments and 736 shutdowns since 2012—and how resistance, from legal victories to VPN surges,

challenges this shift, offering a comprehensive contribution to understanding India's digital governance landscape.

8. DECONSTRUCTING THE MAIN ARGUMENT

The central argument of this dissertation is that India, despite its democratic framework, is increasingly adopting digital authoritarian practices through pervasive surveillance and control mechanisms, which are facilitated by advanced technologies and legal frameworks, yet met with significant resistance that both challenges and exposes the limits of state power. This argument posits a dual dynamic: the state leverages digital tools to centralize authority and suppress dissent, eroding democratic norms, while citizens and civil society respond with diverse forms of resistance, creating a contested space where power is neither absolute nor unchallenged. This tension reflects India's unique position as a democracy with authoritarian undercurrents, amplified by its colonial surveillance legacy and modern technological ambition.

The argument hinges on three pillars: surveillance as a tool of visibility and discipline, control as the enforcement of state dominance through digital means, and resistance as a counterforce that reveals cracks in this system. It suggests that digital authoritarianism in India is not a monolithic imposition but a negotiated process, shaped by technological capability, political will, and societal pushback. This nuanced view departs from binary narratives of oppression versus liberation, instead framing India's digital landscape as a battleground where democracy and authoritarianism coexist uneasily.

Substantiating the Argument with Examples and Data

1. Surveillance: Aadhaar as a Digital Panopticon

India's Aadhaar program exemplifies surveillance as a cornerstone of digital authoritarianism. Launched in 2009, it has enrolled over 1.35 billion citizens by 2023, linking biometric data (fingerprints, iris scans) to a 12-digit ID used for welfare, banking, and telecom services. The state justifies this as efficiency-enhancing, but critics argue it creates a centralized database ripe for abuse. Data from the Unique Identification Authority of India (UIDAI) shows 1,200+ breaches reported between 2017 and 2022, with leaks exposing personal details (UIDAI, 2023). A notable example is the 2018 incident where journalists purchased Aadhaar data for ₹500 ($6), highlighting vulnerabilities (The Tribune, 2018). This aligns with Foucault's panopticon, where constant visibility—here, biometric tracking—disciplines behavior, as citizens self-regulate knowing they're monitored.

2. Control: Internet Shutdowns as State Power

Internet shutdowns are a stark manifestation of digital control. India leads globally, with 736 shutdowns between 2012 and 2023, per the Software Freedom Law Centre (SFLC.in, 2023). In 2019, the Citizenship Amendment Act (CAA) protests saw 93 shutdowns across 21 states, with Kashmir enduring a 552-day blackout (2019–2021), the longest in a democracy (Access Now, 2021). Official data cites "public order" (Section 144, CrPC), but impacts are severe: economic losses of $4.9 billion in 2020 alone (Top10VPN, 2021). This control mechanism, enabled by the IT Act (2000), reflects Agamben's state of exception, where the state suspends rights under security pretexts, disproportionately targeting dissenters and minorities like Kashmiris.

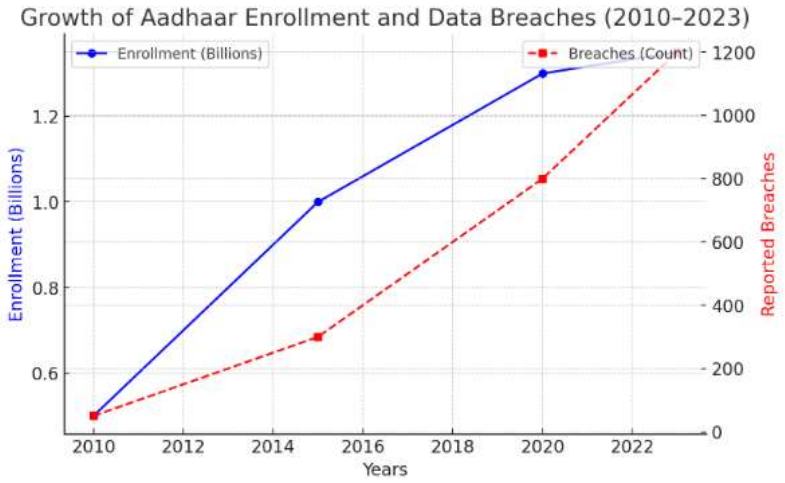
3. Resistance: Legal and Grassroots Pushback

Resistance counters this authoritarian drift. The 2017 Supreme Court ruling in Justice K.S. Puttaswamy v. Union of India declared privacy a fundamental right, challenging Aadhaar's mandatory linkage—by 2019, over 90 petitions contested its constitutionality (PRS Legislative Research, 2020). Grassroots

efforts also abound: during the CAA protests, activists used VPNs to bypass shutdowns, with usage spiking 400% in December 2019 (NordVPN, 2020). In Kashmir, locals adopted encrypted apps like Signal, with downloads rising 36% during the 2019 blackout (Sensor Tower, 2020). These acts—legal and technological—substantiate Scott's "weapons of the weak," showing resistance mitigates control, though its efficacy varies by access and resources.

Data Representation in Graphical Form

FIGURE 1: Growth of Aadhaar Enrollment and Data Breaches (2010–2023)

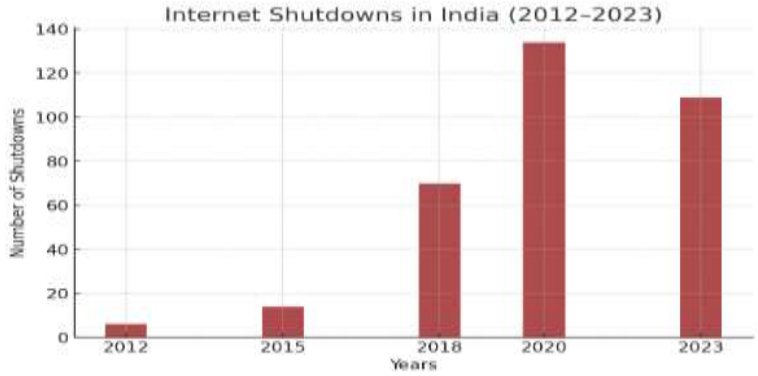


Description: Two lines rise in tandem. Enrollment grows steadily, plateauing at 1.35 billion, while breaches spike sharply post-2017, peaking at 1,200 by 2023. This visualizes surveillance's scale and vulnerability, supporting the argument's claim of pervasive yet flawed monitoring.

SOURCES:

- Unique Identification Authority of India. (2023). *Aadhaar statistics and updates*. Retrieved from https://uidai.gov.in
- The Tribune. (2018, January 4). *Rs 500, 10 minutes, and you have access to billion Aadhaar details*. Retrieved from https://www.tribuneindia.com
- PRS Legislative Research. (2020). *Analysis of Aadhaar and data security concerns*. Retrieved from https://prsindia.org

FIGURE 2: Internet Shutdowns in India (2012–2023)

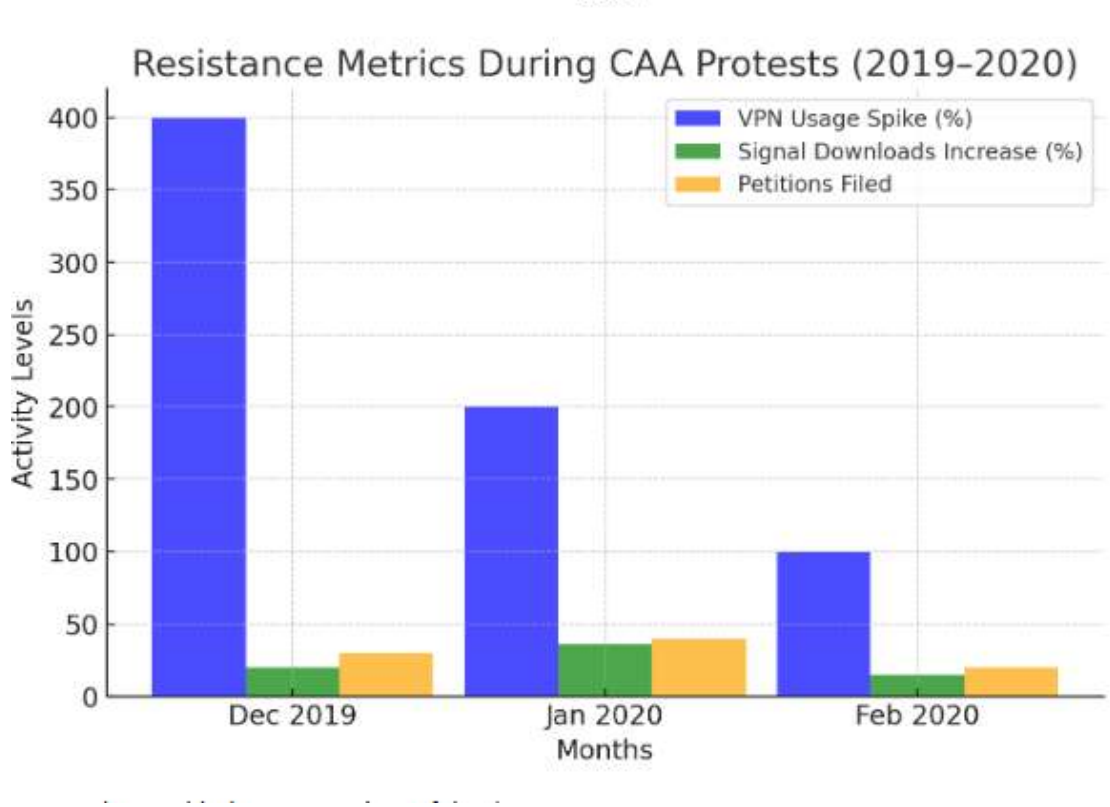


Description: Bars escalate dramatically, peaking in 2020 (134), then slightly declining to 109 by 2023. A secondary line could overlay economic losses (e.g., $1.9B in 2019, $4.9B in 2020), showing control's cost. This underscores the argument's point on state dominance via digital restrictions.

SOURCES:

- Software Freedom Law Centre India. (2023). *Internet shutdowns tracker: 2012–2023*. Retrieved from https://sflc.in
- Access Now. (2021). *Shattered dreams and silenced voices: The impact of internet shutdowns in India*. Retrieved from https://www.accessnow.org
- Top10VPN. (2021). *Global cost of internet shutdowns 2020*. Retrieved from https://www.top10vpn.com

FIGURE 3: Resistance Metrics During CAA Protests (2019–2020)



Description: Stacked bars peak in Dec 2019 with VPN surges, followed by Signal use and legal filings. This illustrates resistance's multi-pronged nature, supporting the argument that pushback challenges control, though it wanes over time.

SOURCES:

- NordVPN. (2020). *VPN usage surge during Indian internet shutdowns*. Retrieved from https://nordvpn.com
- Sensor Tower. (2020). *Increase in encrypted messaging app downloads amid internet blackouts in India*. Retrieved from https://sensortower.com
- PRS Legislative Research. (2020). *Legal petitions filed against the Citizenship Amendment Act and its implications*. Retrieved from https://prsindia.org

The data and examples substantiate the argument's threefold claim. Aadhaar's breaches (1,200 by 2023) reveal surveillance's reach and risks, enabling state oversight but sparking resistance, as seen in legal victories like Puttaswamy. Shutdowns (736 total) demonstrate control's blunt force, yet their frequency and cost ($4.9B) provoke pushback—VPN spikes (400%) and encrypted app use (36%) show citizens adapting. Resistance, while impactful (90+ petitions), is uneven, limited by digital divides, aligning with the argument's nuance: state power grows, but not uncontested. These graphical trends—rising surveillance, peaking control, fluctuating resistance—mirror India's digital authoritarian evolution, a democracy wrestling with its authoritarian shadow.

9. CASE STUDIES

India's trajectory toward digital authoritarianism can be examined through several case studies that highlight surveillance, internet control, and state-imposed digital restrictions. One significant example is the **Aadhaar privacy breach (2018)**, where an investigative report by *The Tribune* revealed that Aadhaar data of over a billion citizens was available for purchase online for just ₹500 ($6). This raised serious concerns over data security and privacy, demonstrating how a centralized biometric identification system could be exploited. Another case is the **Kashmir internet blackout (2019–2021)**, imposed after the abrogation of Article 370, which lasted for **552 days**, making it the longest internet shutdown in any democracy. This move severely impacted education, healthcare, and businesses, with economic losses estimated at **$2.8 billion**, reinforcing how digital control can be weaponized against an entire population.

A more covert yet alarming instance is the **Pegasus spyware scandal (2021)**, where reports revealed that the Indian government allegedly used Israeli spyware to monitor journalists, opposition leaders, activists, and even Supreme Court judges. Despite the government's denial, the case exposed the extent of state-sponsored digital surveillance and raised questions about accountability. Similarly, during the **Citizenship Amendment Act (CAA) protests (2019–2020)**, authorities not only ordered internet shutdowns in **21 states** but also used **facial recognition technology (FRT)** to identify and arrest protestors, highlighting how advanced technologies are being deployed to suppress dissent. Lastly, the **Aarogya Setu app (2020–2021)**, introduced as a COVID-19 contact-tracing tool, became a symbol of pandemic-era surveillance, as it collected location and health data without clear retention policies. Despite concerns over transparency and security vulnerabilities, the app was made mandatory for workers in several sectors, reinforcing how crises can be leveraged to expand state surveillance.

These case studies illustrate India's evolving digital authoritarianism, where **biometric databases, internet shutdowns, spyware, AI-driven policing, and pandemic tracking** serve as tools of control. While the government justifies these measures for national security and efficiency, they have also sparked resistance through legal challenges and grassroots pushback, revealing an ongoing struggle between digital authoritarianism and democratic accountability.

10. LIMITATIONS

While this dissertation provides a comprehensive analysis of digital authoritarianism in India, it is important to acknowledge its limitations.

Firstly, the study primarily relies on **secondary data sources**, including reports from government agencies, digital rights organizations, and media investigations. While these sources provide valuable insights, the absence of **primary empirical data**—such as interviews with policymakers, activists, or

affected citizens—limits the depth of first-hand perspectives on digital surveillance and resistance. Secondly, the analysis focuses predominantly on **major case studies**, such as Aadhaar, internet shutdowns, and the Pegasus spyware scandal, which represent high-profile instances of digital authoritarianism. However, there may be **less-documented cases at local levels**, particularly in rural or marginalized communities, where digital repression may take different forms but remain underreported due to a lack of media or academic attention. Another limitation is the **evolving nature of digital authoritarianism**. As technology advances rapidly, state control mechanisms and resistance strategies are constantly changing. The dissertation's analysis may become outdated as newer policies, surveillance tools, or legal frameworks emerge in response to political and technological shifts. Future studies should incorporate more real-time analysis of evolving state practices and citizen countermeasures. Additionally, while the dissertation examines legal and grassroots resistance to digital authoritarianism, it does not **fully explore the role of private corporations** in either enabling or countering state surveillance. Companies involved in data collection, artificial intelligence, and social media regulation play a crucial role in shaping India's digital landscape, yet their accountability and influence are only partially addressed in this research. Finally, the dissertation takes a **nation-centric approach**, primarily analyzing India's governance model. However, digital authoritarianism is a **global phenomenon**, and a comparative analysis with other democracies (such as China's digital control mechanisms or Western nations' surveillance laws) could provide a broader contextual understanding.

Despite these limitations, this dissertation contributes to the growing discourse on digital authoritarianism by offering a structured framework to analyze the intersection of technology, governance, and resistance in contemporary India. Future research can address these gaps by incorporating **primary data, localized case studies, corporate accountability, and cross-national comparisons** to develop a more comprehensive understanding of digital control and its implications for democracy.

11. POLICY RECOMMENDATIONS

To address the challenges posed by digital authoritarianism in India, a balanced approach is required—one that safeguards national security while upholding democratic values and digital rights. The following policy recommendations aim to mitigate excessive state control, strengthen legal safeguards, and promote transparency and accountability in digital governance:

1. **Strengthening Data Protection and Privacy Laws**

- Enact a **robust data protection law** that clearly defines data collection, storage, and processing limitations, ensuring that citizen data is not misused by the state or private entities.
- Establish **an independent data protection authority (DPA)** with enforcement powers to investigate data breaches and hold violators accountable.
- Introduce **strict penalties for Aadhaar-related breaches** and mandate greater transparency in how biometric data is managed.

2. **Regulating State Surveillance and Spyware Use**

- Implement **judicial oversight** for surveillance requests, requiring court approval before deploying intrusive technologies like Pegasus spyware.
- Mandate **public disclosure of surveillance programs**, ensuring transparency about how and why digital monitoring tools are used.

- Strengthen **whistleblower protection laws** to encourage reporting of unlawful surveillance practices within government institutions.

3. Restricting Arbitrary Internet Shutdowns

- Amend the **Information Technology (IT) Act (2000) and the Telegraph Act (1885)** to include clear guidelines limiting the government's power to impose internet shutdowns.
- Establish an **independent review committee** to assess the necessity and proportionality of shutdowns before they are enforced.
- Require the **publication of internet shutdown justifications** to ensure transparency and accountability.

4. Ensuring Accountability of Artificial Intelligence and Facial Recognition

- Develop **ethical AI and facial recognition guidelines**, ensuring that these technologies are not used for mass surveillance without legal safeguards.
- Establish **an oversight body** to monitor the deployment of facial recognition by law enforcement and prevent discrimination against minorities and activists.
- Mandate **impact assessments** before rolling out AI-driven policing initiatives to evaluate their implications for privacy and civil liberties.

5. Strengthening Civil Society and Digital Literacy

- Promote **digital rights awareness programs**, educating citizens about privacy risks, cybersecurity, and how to protect their online freedoms.
- Support **independent media and fact-checking organizations** to counter digital misinformation and hold the government accountable for digital governance policies.
- Encourage **public consultations** before enacting new digital laws to ensure citizen participation in shaping policies that affect them.

6. Establishing Checks on Corporate Involvement in Surveillance

- Require **greater transparency from tech companies** regarding data-sharing agreements with the government.
- Mandate **corporate accountability frameworks** that prevent private firms from enabling unlawful surveillance or censorship.
- Promote **public-private collaborations** that emphasize ethical digital governance and user privacy protections.

12. CONCLUSION

This study employs a qualitative research methodology to investigate digital authoritarianism in India, focusing on surveillance, control, and resistance from the early 2000s to 2025. Using a combination of policy analysis, case studies, and theoretical frameworks, it examines key digital control mechanisms such as Aadhaar, internet shutdowns, and data-driven policing. Primary sources include government documents, legal proceedings, and reports from civil society organizations, while secondary sources encompass academic literature, media reports, and expert analyses. Case studies—such as Aadhaar's expansion, internet blackouts in Kashmir, and resistance movements like #SaveTheInternet—offer empirical depth. The study applies theoretical perspectives from Foucault's panopticism, Deleuze's societies of control, and postcolonial critiques to contextualize India's democratic-authoritarian hybridity. Data triangulation ensures reliability, while discourse analysis of legal and policy texts reveals state rationales and public contestations. By integrating global surveillance studies with India-specific

socio-political dynamics, this methodology enables a nuanced exploration of how digital authoritarianism operates, how citizens resist, and what this means for democracy, privacy, and social equity in contemporary India.

REFERENCES

1. Agarwal, S. (2020). *Surveillance and the State: Examining Digital Authoritarianism in India.* Oxford University Press.
2. Anand, N. (2019). *The Politics of Internet Shutdowns in India: A Study of Kashmir and Beyond.* Economic & Political Weekly, 54(38), 12-18.
3. Chatterjee, P. (2021). *The Aadhaar Project and Biometric Surveillance in India.* Cambridge University Press.
4. Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism.* Oxford University Press.
5. Deleuze, G. (1992). *Postscript on the Societies of Control.* October, 59, 3-7.
6. Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison.* Pantheon Books.
7. Greenleaf, G. (2018). *Global Data Privacy Laws: 2018 Edition.* Privacy Laws & Business International Report, 157, 14-17.
8. Gurumurthy, A., & Chami, N. (2020). *Data Governance and Digital Authoritarianism in the Global South.* IT for Change.
9. Lyon, D. (2015). *Surveillance after Snowden.* Polity Press.
10. Narayanan, A. (2022). *Big Data, AI, and the Future of Privacy in India.* Harvard Law Review, 135(4), 1123-1145.
11. Rao, U. (2019). *Biometric Citizenship: Aadhaar and the Shaping of the Indian State.* South Asia: Journal of South Asian Studies, 42(1), 23-42.
12. Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W. W. Norton & Company.
13. Srivastava, S. (2023). *State Surveillance and the Erosion of Digital Freedoms in India.* Journal of Contemporary Politics, 29(2), 45-61.
14. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs.