BIPSS Commentary
www.bipss.org.bd March-2026
BIPSS Towards a Secure World

The Algorithmic State: Are We Sleepwalking into Digital Authoritarianism?

Nabib Bin Zahid[1]

Source: TecScience[2]

Introduction

The term "algorithmic state" describes a kind of government where automated, data-driven technologies are increasingly in charge of making decisions. Large datasets are analyzed by these systems in order to implement or influence policies in a variety of fields, including information control, welfare distribution, and police. Algorithmic systems radically change the way power is used, moving it from obvious institutional players to opaque technical infrastructures, even though they are sometimes presented as instruments for efficiency and impartiality.

Digital authoritarianism, on the other hand, refers to the use of digital technology, particularly big data analytics, artificial intelligence, and surveillance systems, to monitor, manage, and influence populations in ways that support centralized power. Digital authoritarianism functions through subtle, ongoing, and sometimes undetectable techniques ingrained in commonplace technical systems, in contrast to earlier authoritarian governments that depended on overt force.

This commentary contends that the expansion of algorithmic control, along with limited regulatory monitoring and entrenched power disparities, produces structural conditions favorable to digital dictatorship. This transition is not often purposeful; rather, it arises gradually via the normalization

[1] Nabib Bin Zahid is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). He has completed his B.S.S in International Relations from the University of Rajshahi.
[2] https://tecscience.tec.mx/en/science-communication/algorithmic-governance/

of monitoring, the automation of decision-making, and the degradation of institutional responsibility.

The issue is especially relevant in today's socio-political climate, when both governments and companies rely significantly on algorithmic systems to manage complexity. According to Shoshana Zuboff, the collection and analysis of behavioral data has become crucial to modern power systems, changing the interaction between individuals and institutions.[3] The implications are profound: governance is increasingly mediated by systems that lack transparency, challenge accountability, and concentrate power in unprecedented ways.

From Bureaucratic Control to Algorithmic Governance

Modern governance has always been intertwined with systems of information management. Early bureaucratic states relied on censuses, registries, and statistical tools to categorize and control populations. These systems laid the groundwork for what David Lyon terms the "surveillance society," in which monitoring becomes a routine aspect of governance.[4]

Technological mediation of governance intensified in the 20th century. Early computational tools, such as punch-card systems, enabled governments to process large volumes of population data efficiently. While these systems were initially developed for administrative purposes, they demonstrated how technological infrastructures could amplify state power. Historical evidence shows that such systems were later repurposed for more coercive forms of control, highlighting the dual-use nature of data technologies.

Source: The Regulatory Review[5]

Authoritarian regimes have consistently leveraged available technologies to consolidate power. Radio and film were used extensively for propaganda, while secret police networks relied on

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: PublicAffairs, 2019).
[4] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001)
[5] https://www.theregreview.org/2025/12/15/livermore-the-political-limits-of-algorithmic-governance/

surveillance and informants to suppress dissent. However, these systems were constrained by human limitations - data processing was slow, and surveillance required significant manpower.

The digital revolution eliminated many of these constraints. The rise of the internet, mobile technologies, and big data analytics enabled real-time data collection and analysis on an unprecedented scale. Following the events of September 11, 2001, governments significantly expanded surveillance capabilities under the justification of national security[6], which normalized large-scale data collection, often with limited transparency or oversight.

These historical patterns reveal a consistent trajectory which shows technologies introduced for efficiency or security tend to expand into tools of control when embedded within unequal power structures. The current shift toward algorithmic governance reflects this trajectory but with significantly greater intensity due to the scale, speed, and opacity of contemporary systems.

The Global Architecture of Algorithmic Control

Surveillance Systems and Predictive Governance

Contemporary states increasingly deploy algorithmic surveillance systems to monitor populations. Technologies such as facial recognition and predictive analytics enable real-time tracking and behavioral analysis. According to Freedom House, artificial intelligence is now widely used by governments to enhance surveillance and automate social control mechanisms.[7]

Source: Brookings[8]

Predictive policing systems exemplify this trend which analyzes historical crime data to forecast potential criminal activity. Presented as neutral tools, they often reproduce existing biases

[6] Carly Nyst, Tomaso Falchetta, The Right to Privacy in the Digital Age, *Journal of Human Rights Practice*, Volume 9, Issue 1, February 2017, Pages 104–118, https://doi.org/10.1093/jhuman/huw026

[7] Funk, Allie, Adrian Shahbaz, and Kian Vesteinsson. "The repressive power of artificial intelligence." Freedom House (2023).

[8] https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

embedded in the data. Cathy O'Neil argues that such systems can create self-reinforcing cycles of discrimination, disproportionately targeting marginalized communities.[9]

Algorithmic Control of Information Ecosystems

Algorithmic control of information ecosystems involves the methodical structuring of exposure, attention, and eventually perception rather than just content filtering. Social media sites like Facebook, YouTube, and TikTok don't offer unbiased information. They use engagement-optimized ranking algorithms to construct personalized worlds. information that increases user retention is given priority by this optimization logic, which frequently amplifies information that is sensational, divisive, or emotionally charged.[10] What emerges is not just a distortion of information, but a reconfiguration of the informational environment itself.

What researchers refer to as algorithmic curation is at the heart of this approach. Algorithms predict user preferences and present content in accordance with them, as opposed to users actively choosing information. According to Tarleton Gillespie, these systems serve as "custodians of the internet's public discourse," subtly incorporating institutional goals like expansion and profitability into the visible architecture.[11] This introduces a structural bias: content that aligns with engagement metrics is systematically privileged, while dissenting, nuanced, or less "performative" voices are often marginalized.

Source: Brookings[12]

There are important ramifications for political communication. Algorithmic amplification can exacerbate ideological echo chambers, according to empirical studies. Eli Pariser's idea of the

---

[9] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown, 2016).

[10] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

[11] Tarleton Gillespie, "The Relevance of Algorithms," in *Media Technologies: Essays on Communication, Materiality, and Society*, ed. Tarleton Gillespie, Pablo Boczkowski, and Kirsten Foot (Cambridge, MA: MIT Press, 2014), 167–194

[12] https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

"filter bubble" encapsulates how users' preexisting opinions are reinforced by tailored feeds that insulate them from alternative viewpoints.[13] More recent studies extend this concern, demonstrating that recommender systems can actively guide users toward more extreme content over time - a phenomenon sometimes described as "algorithmic radicalization."[14] While platforms dispute the extent of this effect, internal documents and independent audits suggest that engagement-driven systems frequently privilege divisive content because it sustains attention.

The opacity of these systems exacerbates the issue. The majority of platforms prohibit external examination by treating their algorithms as confidential. This is a "black box" issue, according to Frank Pasquale, as processes that influence public opinion are opaque and difficult to challenge.[15] This opacity creates a governance gap - platforms wield quasi-regulatory power over speech without the accountability mechanisms typically associated with public institutions.

These algorithmic infrastructures are increasingly being used by state actors. Governments can use coordinated misinformation operations that manipulate algorithmic ranking systems, exert pressure on platforms to delete or conceal specific narratives, or influence content moderation rules. As a result, corporate and governmental interests coexist inside the same data infrastructure in a hybrid control model. Freedom House reports show how governments in many countries utilize digital platforms for narrative control in addition to monitoring, frequently using platform algorithms to magnify messages that support the state.[16]

From a governance perspective, this represents a shift from direct control of speech to control of informational conditions. The distinction is critical. Traditional censorship is visible and contestable; algorithmic control is diffuse and often imperceptible. Yet its effects may be more profound, as it operates continuously and at scale, structuring the epistemic environment within which political and social judgments are formed.

The strategic risk is clear: when informational ecosystems are governed by opaque algorithms optimized for engagement and susceptible to political influence, the integrity of public discourse becomes fragile. The issue is not merely misinformation or bias - it is the systemic reengineering of how societies produce, distribute, and validate knowledge.

---

[13] Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (New York: Penguin Press, 2011).
[14] Zeynep Tufekci, "YouTube, the Great Radicalizer," *The New York Times*, March 10, 2018.
[15] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).
[16] Freedom House, *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence* (Washington, DC: Freedom House, 2023).

Global Convergence Toward Algorithmic Governance: Different Regimes, Same Infrastructure

The growth of algorithmic governance is frequently presented as a phenomenon exclusive to authoritarian or technologically advanced nations. The way it is framed is deceptive. In reality, a global convergence is taking place: nations with very diverse political systems are using remarkably comparable computational tools to regulate, optimize administration, and manage people. The difference is more in how aggressively and publicly the technology is used than in the technology itself.

Efficiency, security, and scalability are the three common imperatives that are driving this convergence at the structural level. Algorithmic systems provide a means for governments to digest information and take large-scale action in the face of growing complexity, including urbanization, migration, and economic instability. As a result, governance structures throughout the world are incorporating technologies like automated decision-making, biometric identification, and predictive analytics.[17] What begins as administrative modernization often evolves into deeper forms of behavioral monitoring and control.

A useful way to test this trend is to compare different governance contexts. In more overtly authoritarian systems, algorithmic technologies are deployed explicitly for social control. Large-scale surveillance infrastructures, including facial recognition and real-time data integration, are used to monitor populations and preempt dissent.[18] These systems are often centralized, with minimal legal constraints, allowing for rapid expansion and integration across domains such as policing, finance, and mobility.

However, focusing exclusively on such cases obscures a more subtle but equally significant dynamic within democratic states. Here, algorithmic governance is typically introduced under the banners of innovation, efficiency, or public service improvement. Automated welfare systems, risk-scoring tools in criminal justice, and algorithmic content moderation on digital platforms are framed as neutral or technical solutions.[19] Yet, despite the difference in rhetoric, the underlying logic is comparable: decisions that affect rights and opportunities are increasingly delegated to opaque systems.

Empirical research supports this concern. Studies show that algorithmic decision-making in areas such as policing and welfare disproportionately affects marginalized populations, often replicating

---

[17] Rob Kitchin, "Thinking Critically about and Researching Algorithms," *Information, Communication & Society* 20, no. 1 (2017): 14–29.

[18] Freedom House, *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence* (Washington, DC: Freedom House, 2023).

[19] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018).

and amplifying existing inequalities.[20] These outcomes are not necessarily the result of intentional repression but of systemic biases embedded within data and model design. Over time, such systems can normalize unequal treatment under the guise of technical objectivity.

Another dimension of convergence is the increasing role of private technology firms in governance. Governments often lack the technical capacity to develop complex algorithmic systems in-house, leading to partnerships with large technology companies.[21] This creates a hybrid governance model in which public authority is partially outsourced to private actors. The implications are significant: decision-making processes become less transparent, accountability is diffused, and profit motives intersect with public policy objectives.

Convergence is further accelerated by cross-border dissemination. Technologies created in one setting are quickly adopted in another, sometimes without giving local legal or ethical frameworks any thought. For example, AI-powered surveillance technologies and biometric identification systems being sold throughout the world, occasionally to governments with lax human rights laws. As a result, innovative methods in one jurisdiction become commonplace in another, creating a feedback cycle.

The critical point is that convergence does not require coordination. It emerges organically from shared incentives, technological standardization, and policy diffusion. This makes it more difficult to resist, as it is not driven by a single actor or ideology but by a broader structural shift in how governance is conceived and executed.

From a strategic standpoint, the real risk lies in complacency. Because algorithmic governance is often introduced incrementally—one system at a time—it does not trigger the same level of scrutiny as more visible political changes. Yet, as these systems accumulate, they can fundamentally reshape governance. The endpoint is not necessarily a classical authoritarian regime, but a hybrid system in which control is exercised through technical infrastructures that operate beyond meaningful public oversight.

Implications for Society

Erosion of Privacy and Autonomy

The expansion of algorithmic governance has far-reaching implications that extend beyond technical efficiency. At its core, it reshapes the relationship between individuals and institutions. Continuous data collection erodes personal privacy, transforming individuals into constant subjects of monitoring. As Lyon opines that surveillance becomes embedded in everyday life,

[20] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown, 2016).
[21] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

often operating without explicit consent, creating a chilling effect where individuals modify behavior due to perceived observation.[22]

Source: The Digital Speaker[23]

Algorithmic Bias and Structural Inequality

Although algorithmic systems are generally portrayed as impartial and objective, in reality, they can magnify and embed preexisting societal injustices. This happens as a result of algorithms being trained on past data that shows deeply ingrained discriminatory habits. Biased results are consistently replicated when such data is used without critical correction.

Source: The New York Times[24]

[22] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001).
[23] https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/
[24] https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html

Predictive policing, in which computers trained on past arrest data disproportionately target populations that are already overpoliced, is a well-documented example. These techniques create a feedback cycle of monitoring and enforcement by reinforcing previous policing behaviors rather than objectively recognizing criminality.[25] Similarly, automated welfare systems have been shown to penalize low-income individuals through error-prone risk scoring and fraud detection mechanisms, often resulting in wrongful benefit denials.[26]

Hiring algorithms also exhibit bias, as machine learning models trained on historical hiring data have duplicated racial and gender gaps by giving preference to applicants who resemble historically dominant groups.[27] These examples show that algorithmic bias is systemic rather than inadvertent, ingrained in data, design, and implementation. Because judgments are hidden behind intricate technical systems, the result is a type of inequity that is scalable, systematic, and hard to challenge.

Conclusion

The development of the algorithmic state indicates a fundamental change in governance. While algorithmic systems provide apparent benefits in terms of efficiency and scalability, they also create structural circumstances conducive to digital totalitarianism. This piece indicates that the hazards are not speculative, but are based on historical patterns, current practices, and theoretical understanding. The mix of monitoring, automation, and opacity results in a governance paradigm that can damage civil rights, distort democratic processes, and consolidate power.

The future of digital governance is uncertain, but it is obvious in its orientation. Without strong regulatory frameworks, transparency measures, and democratic monitoring, the rise of algorithmic systems may result in a type of government that favors efficiency above freedom.

The central question is whether societies will recognize and address these risks in time—or continue to adopt algorithmic systems uncritically, gradually transitioning into a regime where power is exercised not through visible authority, but through invisible code.

---

[25] Andrew D. Selbst et al., "Fairness and Abstraction in Sociotechnical Systems," *Proceedings of the Conference on Fairness, Accountability, and Transparency* (2019).

[26] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018).

[27] Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104, no. 3 (2016): 671–732.