Research Journal in Advanced Humanities

RJAH

https://doi.org/10.58256/2xm2he28

Open Access

Check for updates

RESEARCH ARTICLE Section: *History*

Algorithmic power in autocratic regimes: Critical analysis for democratic resilience in the digital age

Caroline Paskarina[1]*

[1]Department of Political Science, Faculty of Social and Political Sciences, Universitas Padjadjaran, Indonesia

*Correspondence: caroline.paskarina@unpad.ac.id

ABSTRACT

This article examines the influence of algorithms in the context of digital authoritarianism and their impact on democratic resilience. Drawing on a synthesis of literature, this work addresses political algorithmics, artificial surveillance technologies, and information control through digital gatekeeping. The article highlights the logic of power algorithms as a form of predictive power relations that obscure and automate control. Case studies from Southeast Asian countries, such as Vietnam, Thailand, and Indonesia, illustrate how autocratic governments use algorithms to filter public sentiment, suppress dissent, and control narratives. The analysis reveals three components of algorithmic politics: predictive and personalized automation, repressive algorithms, and manipulation of information systems. These components demonstrate the extent to which algorithmic power reinforces authoritarian rule while simultaneously eroding the foundation of democratic resilience by dismantling the public sphere of reasoned debate, deepening societal divisions, and diminishing the level of critical citizenship and digital civic engagement. The article urgently proposes rethinking the political theory of power to incorporate technological, epistemological, and emotional frameworks in the digital age.

KEYWORDS: AI surveillance, algorithmic politics, democratic resilience, digital authoritarianism, power theory

Research Journal in Advanced Humanities

Volume 7, Issue 2, 2026

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: 09 **March 2026**

Accepted: 03 **May 2026**

Published: 25 **June 2026**

HOW TO CITE

Paskarina, C. (2026). Algorithmic power in autocratic regimes: Critical analysis for democratic resilience in the digital age. *Research Journal in Advanced Humanities*, *7*(2). https://doi.org/10.58256/2xm2he28

Published in Nairobi, Kenya by Royallite Global, an imprint of Royallite Publishers Limited

Introduction

Two decades of uninterrupted technological advancement have given rise to a unique synthesis of dominance focused on algorithms. Algorithmic power refers to the capacity to control and change socio-political activities through automated systems, such as social media, AI, and modern surveillance tools. Rouvroy and Berns (2013) describe algorithms as a new form of power/knowledge that governs populations using data and statistics probabilistically. The initial perception of the internet and the allied digital platforms was that they could usher in an era of information democratization, empowering democratic institutions. The autocratic reality is that such regimes harness these technologies to tighten their control. Digital authoritarianism is described as a paradigm where authoritarian governments utilize information technology to control, manipulate, surveil, and reshape citizens' behaviors through unprecedented repression, censorship, information control, and other politically motivated digital services (Lim, 2025). Experts describe digital authoritarianism as the strategic use of digital information technology by authoritarian regimes to monitor, suppress, and manipulate both domestic and foreign populations(Lim, 2025). The free flow of information does not weaken autocratic regimes; such regimes have weaponized algorithms and information to reinforce their systems of domination. This phenomenon constitutes a monocausal explanation that threatens global democracy and exacerbates the demise of democracy in several nations (Lim, 2025). This finding continues to substantiate the hypothesis that digital technology is not simply a cure for democracy's ills. Such a hypothesis was formulated because the nature of technology is dominantly controlled and utilized by a specialized elite with skills of discrimination and unique mastery over tools. Regardless, this hypothesis seems much more plausible these days, given the current state of politics, where algorithmic politics, employed by political players with undemocratic agendas, heightens socially divisive narratives, creates an infodemic of false information, and promotes autocratic trends (Ünver, 2018).

On a conceptual level, algorithmic power stems from the capability of algorithms to manage information and control sociability at a unique scale (Lim, 2025; Rouvroy & Berns, 2013). Unlike classic authoritarian practices, which rely on manual censorship and media control, digital autocratic regimes exploit the capabilities of big data and AI to automate the presentation of information to the public. Social media algorithms govern which components of user-generated content are presented to users, thus shaping public discourse and opinion in subtle yet profound ways (Ünver, 2018). Recent studies show that the social media algorithm architecture affects the way political messages are disseminated, how information is sought, and even the involvement of citizens in civic life (Lim, 2025; Paskarina, 2023; Paskarina, Hermawati, & Nuraeni, 2021; Ünver, 2018; Wijayanto, Setiyono, Martini, & Elsitra, 2022). Online interactions influenced by automated systems, including bots and trolls, can spread targeted falsehoods to exacerbate political polarization. Automated systems have a significant influence on the political sphere at various levels, including targeted political advertising, voter micro-profiling, mass surveillance using facial recognition technology, and the manipulation of online polls (Ünver, 2018; Wijayanto et al., 2022). This practice shows that software and AI have transcended the state of neutral instruments and become a new power infrastructure. Any actor capable of understanding and deploying such algorithms, be it state agents or technology corporations, exercises enormous political power over the manipulation of behavior.

The urgency of this study topic lies in the significant implications of algorithmic power in digital autocratic regimes for democratic resilience. Democratic resilience refers to the ability of a democratic system to withstand and adapt to challenges or threats. In this context, risks arise from the authoritative use of digital technology (Feldstein, 2021). The surge in AI and algorithm adoption for political control challenges the long-held assumption that automated digital technologies will invariably enhance accountability and participation. Instead, these same digital tools can be strategically used to erode democratic institutions. Comparative research suggests that the spread of information and communication technologies is correlated with democratic backsliding when anti-pluralist political actors hold power (Beacham, Hafner-Burton, & Schneider, 2024; Cevallos, 2025). Countering democracy, whether framed as post-truth politics or the politics of Big Lies, authoritarian regimes justify their rule through the manipulation of context and information. Often, social media algorithms prioritize sensational or emotionally charged content, greatly hindering the spread of truth and profound discourse, while fueling discord and public defamation of government and institutional leaders (Kreps & Jakesch, 2023; Kreps & Kriner, 2023; MacKinnon, 2011). The outcome is a publicly polarized society more willing to surrender freedoms in support of cohesion, a process that weakens resistance and dissent.

In actuality, this steadily undercuts the self-sustaining democratic processes, whereby democratic principles erode while authoritarian rule escalates, bolstered by technological infrastructure. Consequently, a framework is necessary that addresses the ongoing relationship among algorithms, political power, and democracy. This approach combines political technology, focusing on the intersection of algorithms and politics, with the theory of authoritarian versus democratic resilience. The emergence of this approach allows us to analyze the impact of algorithmic dynamics on the contemporary political landscape and the prospects for democratic sustainability.

The literature on digital authoritarianism is mainly developed within the contexts of China, Russia, and post-Soviet countries (Cevallos, 2025; MacKinnon, 2011). This research expands the context by demonstrating how electoral democracies in Southeast Asia, including Indonesia, have also adopted a gradual digital authoritarian logic through the regression of democracy based on digital law (such as the Information and Electronic Transaction Law, content blocking, internet blackouts), the instrumentalization of buzzers and social media algorithms to suppress opposition, and the co-optation of digital platforms without the need to block them (as seen in Vietnam). By highlighting the variety of forms of digital authoritarianism in Vietnam, Thailand, and Indonesia, this research demonstrates that digital authoritarianism is not merely a binary category (authoritarian vs. democratic), but rather an adaptive and contextual spectrum. This research asserts that digital authoritarianism exists in both explicit repressive regimes and electoral democracies, where digital infrastructure is manipulated to maintain power.

Contextually, the Southeast Asian region illustrates the operationalization of algorithmic power in digital autocratic regimes and its challenges to democracy (Wijayanto et al., 2022). The three case studies, namely Vietnam, Thailand, and Indonesia, illustrate a spectrum ranging from full-fledged authoritarian states to democracies facing erosion. In this context, digital technology is a political battleground between state control and citizen resistance. Vietnam exemplifies a stark one-party state that merges strict state control with a global digital platform infrastructure. The Vietnamese government systematically enforces internet censorship and algorithmic regulations to suppress criticism. For instance, Vietnam's Ministry of Information and Communications has required the removal of "malicious" content from social media within 24 hours or even within 3 hours for "highly sensitive" material content (Le, 2021). Consequently, Vietnam is currently one of the countries with the lowest levels of internet freedom in the world, ranking fifth lowest globally according to Freedom House with a score of 22 out of 100 (Funk, Shahbaz, & Vesteinsson, 2024). Over the past decade, the Communist Party of Vietnam has strengthened its control over the digital landscape by amplifying online censorship, imposing prison sentences on netizens who criticize the government, collecting citizen data, and compelling international tech companies like Facebook and Google to adhere to repressive local regulations (Nemo & Larsson, 2022). Through the 2019 Cybersecurity Law, Vietnam mandates that global platforms establish offices in the country, store user data locally, and remove content at the government's request. These measures illustrate the Vietnamese authoritarian regime's capacity to regulate the algorithms of global platforms to impose digital autocracy. This approach sets it apart from the Chinese model, which opts to block foreign platforms entirely (Nemo & Larsson, 2022).

Thailand has shifted from an electoral democracy to digital authoritarianism following the 2014 military coup. Since taking power, the military junta in Thailand has developed one of Southeast Asia's most sophisticated digital surveillance systems (McDermott, 2021). Security forces are equipped with new cyber warfare units and advanced surveillance software, developed in collaboration with foreign companies, capable of comprehensively monitoring citizens' communications. This measure includes intercepting emails and instant messages, secretly activating cell phone cameras and microphones, and tracking the GPS locations of devices (McDermott, 2021). The military rulers have also "militarized" Thailand's cyberspace, transforming it into a digital panopticon where netizens' activities are closely monitored and regulated (McDermott, 2021). The Computer Crime Act and related regulations have been tightened to ensnare critics of the kingdom and the government, as demonstrated by a woman's 43-year prison sentence for a Facebook post deemed to violate lese-majeste (McDermott, 2021). Besides surveillance-based repression, information manipulation by the state is also widespread. The Thai government and military reportedly conducted an organized disinformation campaign following the coup, employing a group of pro-government trolls and buzzers to disseminate a narrative that discredited the opposition movement and pro-democracy activists (McDermott, 2021). This combination of strict censorship, digital surveillance, and algorithmic propaganda enhances the resilience of Thailand's authoritarian

regime while undermining healthy public discourse. For Thailand's vulnerable democracy, these technological challenges complicate efforts to restore the democratic order, as the military authorities have established a long-term control infrastructure in the digital sphere.

Indonesia, as the largest democracy in Southeast Asia, presents a different dynamic: instead of an established autocracy, Indonesia is grappling with the symptoms of digital authoritarianism that are slowly eroding the quality of its democracy. Democratically elected governments can also adopt repressive digital tactics to maintain power. Over the past few years, Indonesia has exhibited a regression trend, in which various state digital instruments have increasingly restricted civil space (Ufen, 2024). The Electronic Information and Transaction Law, along with regulations on hoaxes and hate speech, is often wielded as a legal weapon (lawfare) to silence criticism. Rather than merely protecting against defamation or fake news, these ambiguous articles are systematically used to intimidate and prosecute journalists, activists, and academics who speak out against the oppressive government (Ufen, 2024). The effect is a climate of fear in civil society, where the threat of legal limits on opposition expression is intertwined.

Additionally, political actors in Indonesia utilize "buzzers" and paid cyber forces to manipulate public conversations on social media (Ufen, 2024). This buzzer network operates by promoting pro-government hashtags, attacking political opponents online, and disseminating disinformation that serves the interests of powerful oligarchs. With the assistance of the platform's algorithms (e.g., trends on Twitter or recommendations on Facebook), the content generated by buzzers can reach a broad audience and influence public perception according to their interests, as well as those of the elite (Ufen, 2024). This practice creates the illusion of consent, suggesting that support for government policy is strong, while the frenzy of information engineering conceals critical voices. It is not uncommon for the government to shut down local internet access, as occurred in Papua, to suppress protest mobilizations (Silas, Paskarina, & Herdiansah, 2024). All of these symptoms reflect Indonesian-style digital repression, where legal tools, social media algorithms, and surveillance technology are used in moderate yet consistent doses to control the democratic space. Although Indonesia is not yet an autocracy, the unchecked penetration of algorithmic power risks undermining the long-term resilience of democracy, making it susceptible to electoral authoritarianism.

The above narrative illustrates that combining algorithms, AI, and surveillance technology has opened a new chapter in authoritarian politics that requires critical academic attention. Digital autocratic regimes across various regions, including Southeast Asia, are increasingly adept at using technology to sustain their power, whether through automated content censorship, big data analytics on citizens' behavior, or personalized digital propaganda. The impact on democratic resilience cannot be overlooked: technological advances intended to empower citizens can empower the state to control them instead. Democracy must adapt to this emerging threat. Are democratic institutions and societies capable of developing resilience against adverse algorithmic influences? How should technological governance be approached so democratic values can endure amid the challenges of surveillance capitalism and a new form of Big Brother politics? This critical study addresses these questions by examining algorithmic power mechanisms within digital autocracy and their effects on democratic resilience. Equipped with the aforementioned theoretical framework and lessons learned from Southeast Asian cases, this article will examine how the interplay of algorithms, AI, and surveillance technologies is reshaping power dynamics between citizens in the digital age, as well as their implications for the future of democracy on a global scale. Therefore, this research is expected to make a conceptual and empirical contribution to the Information Technology and Politics literature, particularly in understanding contemporary challenges at the intersection of algorithms, authoritarianism, and democratic resistance.

Methods

This study employs a critical literature review approach to examine how algorithmic power functions within digital autocratic regimes and its impact on democratic resilience. This approach was selected because it enables researchers to not only catalog existing empirical and conceptual findings but also to critique fundamental assumptions, theoretical frameworks, and blind spots in emerging studies (Jesson, Matheson, & Lacey, 2011; Snyder, 2019). This review is more than just descriptive; it serves as a conceptual tool to dismantle the hidden power dynamics and epistemological relationships that shape the production of political knowledge about digital technology. Unlike systematic literature reviews, which emphasize comprehensiveness and replication, a

critical literature review focuses on a reflective, selective, and transformative reading of the existing literature to uncover assumptions, biases, and potential new theoretical contributions in political science and technology studies.

The critical literature review method enables this study to perform a theoretical synthesis of various relevant cross-disciplinary approaches, including political science studies, media and communication studies, digital security studies, and the sociology of technology. The literature reviewed comprises articles from reputable academic journals, scholarly books, and policy research reports from international institutions such as Freedom House, Access Now, and The Citizen Lab, as well as credible field reports and analyses from non-governmental organizations. The literature selection process was conducted purposively, based on its relevance to the core issues in this study: algorithmic power, digital authoritarianism, the transformation of state-citizen relations through technology, and democratic participation resilience.

The review identifies primary sources through academic databases, including Scopus, Mendeley, and Google Scholar. The keywords utilized in the literature search include algorithmic governance, AI and authoritarianism, digital surveillance, democratic resilience, digital repression, and platform politics. The literature of the last decade has been the primary focus for capturing cutting-edge developments. However, some classic texts by thinkers such as Michel Foucault (Collier, 2009; Lemke, 2002), Shoshana Zuboff (2019), and Manuel Castells (2003) are also used as theoretical references to reframe this new development.

The next stage is the thematic synthesis process, in which the selected literature is qualitatively analyzed by grouping the main findings into several major themes, namely are: first, the logic of algorithmic power in the context of authoritarianism; second, the technology of surveillance and the centralization of information power; third, algorithmic mediation of public opinion and deliberative space; and fourth, the implications for democratic resilience. This thematic approach is supported by a critical analysis of the assumptions and frameworks that underlie the arguments in each study, including how power is conceptualized and the role of technology understood.

The analysis used the thematic synthesis technique (Thomas & Harden, 2008), identifying patterns, differences, and conceptual relationships in the selected literature. This process is conducted manually through the open coding of the main narrative in each text, which is then categorized into three major themes: first, the prediction and personalization of citizen behavior; second, the automation of repression and supervision; and third, the manipulation of public space through algorithmic information. Each theme is systematically linked to the conceptual framework of algorithmic power (Lim, 2025; Rouvroy & Berns, 2013), digital authoritarianism (Feldstein, 2021; Wijayanto et al., 2022), and democratic resilience (Beacham et al., 2024) to uncover the theoretical gaps and potential renewal of political understanding in the digital age.

As an analytical strategy, this study combines genealogical and discursive readings of the power narrative in these studies, with an emphasis on how digital technology is positioned as both a subject of governance and an instrument of rule. The perspective of Michel Foucault's theory of governmentality (Dean, 2010; Lemke, 2002) serves as the primary conceptual framework for analyzing how digital technology functions not only as an administrative tool but also as a normative instrument that shapes the subjectivity of citizens. This approach also allows for exploring forms of resistance, counter-conduct, and democratic power that persist under the pressure of hegemonic algorithmic logic.

In a geographical context, this study focuses on case studies in Southeast Asia, specifically Vietnam, Thailand, and Indonesia, as concrete examples of the declining spectrum of technology use under both autocratic and democratic governments. Although non-empirical, the study utilizes robust secondary data, including quantitative findings on digital censorship, internet blackouts, and civil liberties indices, to enhance the qualitative analyses and conceptual reflections.

Utilizing this critical literature review approach, the study aims to map existing knowledge about algorithmic power and digital authoritarianism, highlighting epistemological gaps and the need to develop new political theories that explain the complexities of contemporary digital regimes. The demand for a transdisciplinary and reflective theoretical framework is growing increasingly urgent, given the rapid pace of technological innovation and its significant political implications.

Result and Discussion

The findings of this study, obtained through a critical literature review approach, reveal that algorithmic power, artificial intelligence, and surveillance technology have become technical tools that have transformed into power architectures, reshaping the relationship between the state and its citizens. To capture the thematic terrain of the algorithmic power discourse, a visualization of text data in the form of a word cloud, based on the keywords derived from the literature synthesis, was created.

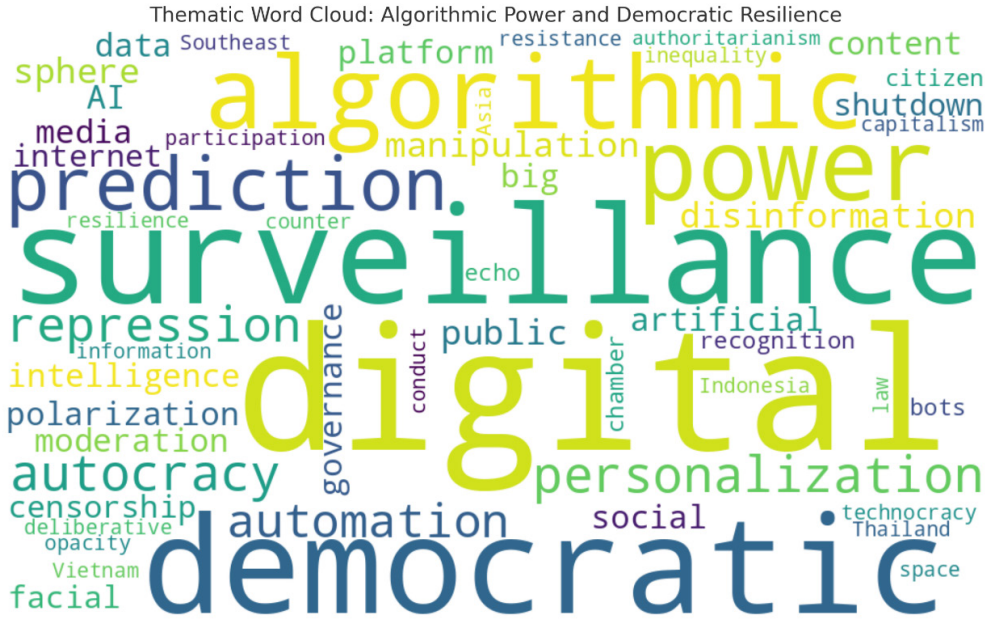

Figure 1. Thematic Word Cloud

The visualization in Figure 1 illustrates the dominant terms in the literature discussing algorithmic power and democratic resilience in Southeast Asia. Terms such as "algorithms", "repression", "disinformation", and "public space" occupy the center of the semantic map, highlighting how digital power has transitioned from the technological to the political realm. The phrases "democratic resilience" and "counter-conduct" suggest an enduring space for resistance that remains relevant for analysis. Within the context of a digital autocratic regime, these dynamics can be categorized into four main themes:

First, prediction and personalization, reflected in the theme of algorithms as predictive power engines. A key aspect of algorithmic power is its capacity to predict individual behavior based on historical data and online activity. In a digital autocracy, algorithms are leveraged to comprehend citizens and anticipate and influence their actions through content curation, micro-targeting, and behavioral nudging (O'Neil, 2016; Zuboff, 2019). In countries like Vietnam and Thailand, social media algorithms promptly and automatically detect anti-government speech and reduce the visibility of such content, directing users to "neutral" information.

This capability grants the state predictive power that was once merely a dream in traditional surveillance. Technologies such as face recognition, biometrics, and big data allow the preemptive screening of "high-risk" individuals prior to any illicit activities being committed (Feldstein, 2021). It obscures the distinction between security measures and political oppression. As exemplified by the mass surveillance program in Xinjiang, similar techniques are beginning to be adopted by Southeast Asian countries, albeit on a more covert and pragmatic scale. The implications for democracy are enormous: algorithmic predictions shift the logic of accountability from a democratic framework to a logic of potential-based control. Citizens are surveilled not just for their activities but also for their potential future behaviors. This measure instills fear and self-censorship, significantly limiting political expression and participation.

Second, the automation of repression relates to the role of AI and platforms in mediating state power. AI and automated systems accelerate the state's administrative processes and transform how power is exercised through automated content moderation, real-time surveillance, and social scoring systems. In Thailand, for example, spyware like Pegasus is reportedly being used against activists and journalists, with AI assisting in information filtering and monitoring communication patterns (Access Now, 2022; Poetranto, 2023) Although they are privately owned, global platforms like Facebook, YouTube, and TikTok have contributed to this

automation, as their recommendation systems often prioritize state-aligned narratives over political correctness or informational diversity. In Vietnam, the government is actively negotiating with these global platforms to automatically remove anti-government content, creating an algorithmic alliance between corporations and the state (Le, 2021). This phenomenon gave rise to a new form of power: power is exerted not only by authoritarian figures or governmental organizations, but also through a network of automation embedded throughout the digital architecture of citizens' lives. Power manifests as ambient, imperceptible but profoundly effective in constraining freedom of expression, manipulating public opinion, and obstructing alternative political agendas. Third, hidden power and organized disinformation are operated through the algorithmic manipulation of public space. Information control in the algorithmic age is exerted through censorship and surveillance, alongside massive content production designed to frame a specific political narrative. In Indonesia, buzzer networks and bots have become crucial in regulating trending algorithms, spreading disinformation, and creating the illusion of majority consent, which enables the government (or certain political actors) to inundate public space with content that corners the opposition and glorifies the government. Meanwhile, algorithmic curation systems either silenced or disregarded criticism (Nugroho, Siregar, & Laksmi, 2022).

Research indicates that platform algorithms tend to favor emotionally charged and contentious material due to its high interaction levels. Authoritarian entities exploit this circumstance to create a digital echo chamber that exacerbates social division and undermines the deliberative capacities of individuals. As a result, the democratic public sphere, designed for logical discourse and the exchange of ideas, devolves into a manipulative algorithmic warfare. In this context, algorithmic power is subtle yet profound; it is not conventionally repressive but reshapes society's cognitive landscape in ways that uphold the status quo. Democracy, which relies on information transparency and equitable access to ideas, is jeopardized when computational frameworks exacerbate narrative disparities. These findings suggest that democracy is facing an epistemic and affective crisis, intensified by the logic of algorithms. The inclination of countries to harness AI and big data for efficiency and security often lacks balance with transparent, accountable, and participatory governance. In Southeast Asia, digital technology is accelerating the fragmentation of civil society and diminishing citizens' critical digital engagement literacy (Tapsell, 2021).

Furthermore, increasingly closed algorithmic surveillance models create a gap between citizens and state institutions. When data-based decision-making becomes opaque, the legitimacy of democracy begins to erode. Algorithmic democracy without transparency turns into a technocracy without accountability. Therefore, the future of democracy will be primarily determined by how civil society, academia, and supervisory institutions can intervene in this algorithmic logic of power. Developing a new political theory that understands the state and citizens as dynamic entities, rather than fixed ones, is necessary, given that digital relations are constantly mediated by technological infrastructure.

To strengthen the systematization of the findings, conceptual visualization maps the relationship between the main concepts.

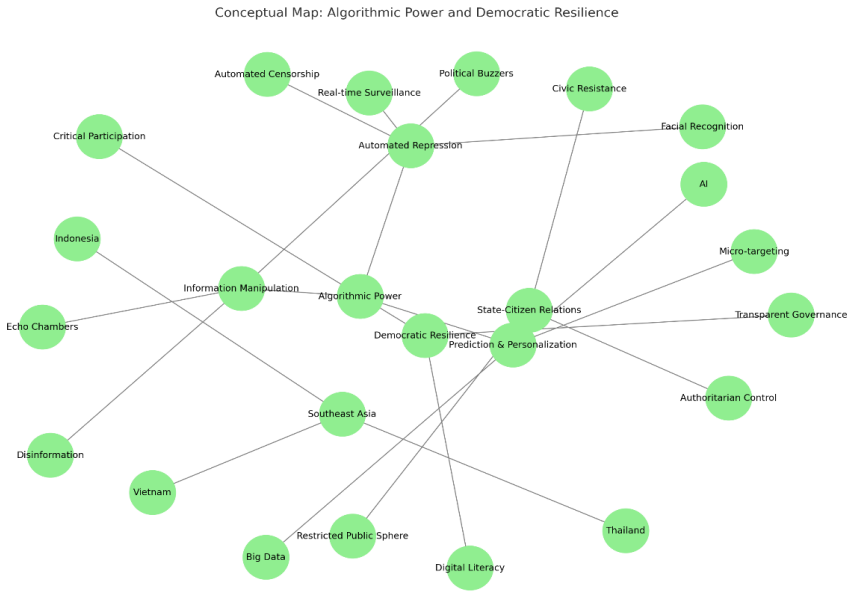

Figure 2. Conceptual Map of Algorithmic Power and Democratic Resilience

Figure 2 illustrates how the three primary mechanisms of algorithmic power relate to changes in state-citizen relations and democratic resilience. Each mechanism is grounded in the digital technology infrastructure integrated into the country's political operations, resulting in new forms of behavior regulation, social repression, and the production of political truth. At the center of this map is "Algorithmic Power," which branches out toward technological practices (prediction, repression, manipulation) as well as political consequences (authoritarian control, citizen resistance, degradation of public space). The final branch leads to democratic resilience, necessitating intervention through digital literacy, critical participation, and transparent governance. This map highlights that algorithmic power functions through three primary mechanisms: prediction and personalization, supported by AI and big data, which enable the state to anticipate citizens' actions even before they occur automatically. Prediction and personalization mechanisms no longer reside solely in the commercial sector but have been embraced by autocratic governance. Countries utilize AI and machine learning to classify citizens, profile potential political risks, and tailor personalized communication interventions, such as notifications, policy offers, or even digital intimidation (Zuboff, 2019). As shown in research by Zuboff (2019) and Feldstein (2021), algorithms not only describe behavior but also unconsciously shape citizens' incentives and choices. In the Vietnamese context, digital reporting and automated censorship systems enable the government to respond to online uploads or expressions before they go viral. The system internalizes state surveillance in citizens' daily activities, transforming them into "algorithmic subjects" that are constantly read, mapped, and directed. This mechanism erodes citizen political agency: if someone feels that the algorithm already "knows" and will "adjust" their online behavior, the desire to voice opinions or organize resistance can weaken even before it emerges.

Second is repression automation, where technology enforces the law and surveillance automatically (facial recognition, real-time monitoring, and automated sensors). The automation of repression creates a form of power that is invisible yet very precise. The use of devices such as facial recognition, real-time GPS surveillance, and AI-driven blocklists enables state repressive actions to be faster, more efficient, and more challenging to track legally. In Thailand, the military's ability to infiltrate civilian digital devices has made political surveillance an integral part of daily cyber operations (Tapsell, 2021). Repression no longer occurs during spectacular moments, such as demonstrations or mass arrests; instead, it manifests through constant monitoring, chilling effects, and algorithmic administrative sanctions, including account deletions, content ranking downgrades, or freezing e-wallets and service access. In this type of system, repression does not necessitate physical violence because "fear" is inherently programmed into the logic of digital systems. Targeted citizens often remain unaware of when or why they are being targeted, inducing political uncertainty that undermines social solidarity and resistance collectivity. This finding expands on the ideas of Rouvroy and Berns (2013) regarding algorithmic governmentality by incorporating a material dimension of algorithmic repression.

The third mechanism is information manipulation, which operates through disinformation and echo chambers created by political buzzers and social media algorithms, unlike the previous two mechanisms that relied on censorship and monitoring. Information manipulation functions within narrative and affective production. With political buzzers, bot farms, and social media platform algorithms, states or pro-regime actors can inundate digital public spaces with content that distorts democratic discourse. In Indonesia, for instance, fake trending hashtags and cyberattacks on the opposition have become a prevalent strategy during critical political moments. Algorithmic recommendation systems amplify pro-government narratives and limit public access to essential information. This practice creates an unequal information structure, where the truth is not determined by validity or rationality, but by the visibility produced by algorithms. The deliberative public space transforms into an automated and strategic propaganda field, constraining citizens' ability to form independent political opinions based on facts.

These three mechanisms establish algorithmic power regimes that operate at structural, affective, and epistemic levels. In this regime, the relationship between the state and citizens becomes asymmetrical, as the state possesses technological advantages and control over the information infrastructure. Citizen resistance becomes increasingly complex to articulate because repression is no longer explicit and measurable but is probabilistic, distributed, and perception-based. Digital public spaces become systematically closed, not due to explicit prohibitions, but by excluding non-conforming content and actors through algorithmic selection logic. The implications for democratic resilience are significant, as they require digital literacy, critical participation,

and transparent governance to thrive in an increasingly unequal and algorithmic ecosystem. The Southeast Asian region is a complex constellation that confirms this dynamic: Vietnam exemplifies total control over the internet, Thailand militarizes the internet, and Indonesia slowly and covertly loses its democratic values. Together, they emphasize that digital autocracy is not inherently equivalent to internet prohibitions or platform restrictions, but rather involves advanced algorithms that perpetuate power disparities inside information infrastructure. To maintain democratic resilience, a new understanding of democracy as a system is needed that relies not only on elections or institutions, but also on the information architecture and technological logic that underpin citizen participation. Democracies that are unable to adapt to these algorithmic challenges will undergo internal erosion, appearing robust on the outside but lacking substance.

The aforementioned data suggest that digital technology has emerged as a new domain for power conflicts. It is not only a means of communication or public service, but a fundamental component of the political framework that dictates who may access information, when, and in what manner. Consequently, democratic resilience in the digital era is achievable only if individuals and democratic institutions can deconstruct, reinterpret, and contest the prevailing algorithmic logic.

Conclusion

This research demonstrates that algorithmic power within digital autocratic regimes has transformed the relationship between the state and its citizens through predictive, automatic, and hidden mechanisms. Based on a critical literature review, it was found that algorithmic power can be recognized through three mechanisms: first, prediction and personalization through algorithms enable the state not only to observe but also to anticipate the behavior of its citizens in real-time, shifting the logic of power from reactive to preventive. Second, the automation of repression, aided by AI and advanced surveillance systems, enhances the state's capacity to exert social and political control without direct human involvement. Third, manipulating information through digital platform algorithms constricts deliberative public spaces, accelerates polarization, and systematically erodes the potential for citizen resistance. This entire mechanism creates structural pressure on democratic resilience by interfering with citizens' access to free and equal information, undermining the integrity of public discourse spaces, and diminishing the critical power of political participation.

In Southeast Asia, case studies from Vietnam, Thailand, and Indonesia reveal various practices of digital authoritarianism. Nevertheless, all exhibit similar patterns concerning the use of technology to reinforce control and suppress dissent. From one-party states to electoral democracies, algorithmic power has proven to be an effective instrument in fostering obedience, obscuring repression, and bolstering the resilience of authoritarian regimes.

These findings significantly contribute to the development of contemporary power theory across three main dimensions: first, the necessity of reconceptualizing power as an implication of algorithmic power practices. Power is now understood not as a direct interaction between the state and its subjects through legal or violent means, but as an integrated digital framework in which algorithms actively mediate, filter, and influence individuals' actions and views. Therefore, these findings expand the Foucaultian notion of governmentality to algorithmic governmentality, wherein control functions through a technical logic that is emotive, predictive, and invisible. The findings elucidate the three main mechanisms of algorithmic power: prediction and personalization, repression automation, and information manipulation, which were previously discussed only in general literature. These three mechanisms reinforce the position of algorithmic power as a fundamental infrastructure of control in contemporary authoritarian regimes, not merely as a tool for the state to use.

Second, the concept of digital authoritarianism must be strengthened. This research enriches the literature on digital authoritarianism by illustrating how algorithms bolster repressive power and reshape the logic of authoritarian legitimacy. Digital authoritarianism no longer relies on overt repression; instead, it operates through the automation of narratives, the normalization of disinformation, and the manipulation of preferences presented as convenience or efficiency.

Third, redefining democratic resilience is essential. In an increasingly complex digital landscape, democratic resilience cannot be adequately assessed solely through institutional indicators or electoral participation. This research highlights the need for a new framework that incorporates epistemic (access to truth), technological

(mastery of digital infrastructure), and affective (citizens' capacity to maintain agency amid algorithms that shape affection and attention).

The findings of this research deepen our understanding of what democratic resilience means in the context of algorithmic power. This understanding can no longer be confined to indicators such as free elections, freedom of the press, or the strength of representative institutions; it must also encompass: epistemic resilience denotes the capacity of citizens to differentiate between valid and false information in a public sphere overwhelmed by algorithmic manipulation; civic resilience is defined as the ability of civil society to maintain spaces for expression, even when the ruling narrative dominates social media and digital platforms; and technological resilience is characterized by the existence of independent actors who can advocate for transparency, create alternative platforms, and address algorithmic inequality.

The research further affirms that democracy can only endure if there is a redistribution of control over technology and information infrastructure, an agenda that has yet to be adequately addressed in the literature on digital democracy. Thus, this article identifies the threats posed by algorithmic power and sets the stage for reformulating theories of political power in the digital age. The need to renew fundamental concepts such as control, freedom, participation, and resistance is becoming increasingly urgent. Amid the strengthened technological logic in governance, politics must be reinterpreted as an arena for competing ideas and an algorithmic field that influences how ideas are accessed, received, and resisted.

Funding:
The research received a grant from Universitas Padjadjaran through the Online Data and Literature Research Grant 2024, grant number 2222/UN6.3.1/PT.00/2024, and the APC was funded with the same grant.

Acknowledgments:
The author would like to thank the University for supporting this research with generous funding and providing publication opportunities through several international conferences to enhance the manuscript.

Conflicts of Interest:
The author declares no conflict of interest.

Disclaimer Statement
This manuscript is not part of a thesis submitted to any university.

Author Biodata
Caroline Paskarina is a senior lecturer at the Department of Political Science and a researcher at the Centre for Political and Democracy Research, Faculty of Social and Political Science, Universitas Padjadjaran.

References

Access Now. (2022, November 15). Pegasus victims sue NSO in Thailand: It's time for spyware accountability - Access Now. Retrieved April 14, 2025, from https://www.accessnow.org/press-release/thailand-pegasus-lawsuit/

Beacham, A., Hafner-Burton, E. M., & Schneider, C. J. (2024). The Weaponization of Information Technologies and Democratic Resilience (No. 9). San Diego, USA. Retrieved from escholarship.org/uc/item/6f24q81x

Castells, M. (2003). The Network Society. Research Policy, 32, 1141–1145. https://doi.org/10.1016/S0048-7333(02)00118-X

Cevallos, A. (2025). How Autocrats Weaponize AI — And How to Fight Back | Journal of Democracy. Retrieved April 13, 2025, from Journal of Democracy website: https://www.journalofdemocracy.org/online-exclusive/how-autocrats-weaponize-ai-and-how-to-fight-back/

Collier, S. J. (2009). Topologies of Power: Foucault's Analysis of Political Government beyond 'Governmentality.' Theory, Culture & Society, 26(6), 78–108. https://doi.org/10.1177/0263276409347694

Dean, M. (2010). Governmentality: Power and Rule in Modern Society. Society, p. 294. https://doi.org/10.5860/CHOICE.47-6521

Feldstein, S. (2021). The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance. Oxford: Oxford University Press.

Funk, A., Shahbaz, A., & Vesteinsson, K. (2024). The Repressive Power of Artificial Intelligence. USA.

Jesson, J. K., Matheson, L., & Lacey, F. M. (2011). Doing Your Literature Review: Traditional and Systematic Techniques. London: Sage.

Kreps, S., & Jakesch, M. (2023). Can AI communication tools increase legislative responsiveness and trust in democratic institutions? Government Information Quarterly, 40(3). https://doi.org/10.1016/J.GIQ.2023.101829

Kreps, S., & Kriner, D. (2023). How AI Threatens Democracy. Journal of Democracy, 34(4), 122–131. https://doi.org/10.1353/jod.2023.a907693

Le, Q. H. (2021). Vietnam's Digital Authoritarianism: The Use of Cyber Surveillance and Online Repression. Journal of Current Southeast Asian Affairs, 40(2), 181–204.

Lemke, T. (2002). Foucault, Governmentality, and Critique. Rethinking Marxism, 14(3), 49–64. https://doi.org/10.1080/089356902101242288

Lim, M. (2025). Social Media and Politics in Southeast Asia (Cambridge; E. Aspinall & M. L. Weiss, Eds.). United Kingdom: Cambridge University Press. https://doi.org/10.1017/9781108750745

MacKinnon, R. (2011). Liberation Technology: China's "Networked Authoritarianism" | Journal of Democracy. Journal of Democracy, 22(2), 32–46. Retrieved from https://www.journalofdemocracy.org/articles/liberation-technology-chinas-networked-authoritarianism/

McDermott, G. (2021, February 17). Thailand's Creeping Digital Authoritarianism – The Diplomat. The Diplomat. Retrieved from https://thediplomat.com/2021/02/thailands-creeping-digital-authoritarianism/

Nemo, B., & Larsson, A. (2022, November 19). The Quiet Evolution of Vietnam's Digital Authoritarianism – The Diplomat. The Diplomat. Retrieved from https://thediplomat.com/2022/11/the-quiet-evolution-of-vietnams-digital-authoritarianism/

Nugroho, Y., Siregar, F., & Laksmi, S. (2022). Digital Disruption in Indonesia's Democracy: Political Buzzer, Disinformation, and Social Media Manipulation. Jakarta: CIPG.

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. In Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. USA: Crown. Retrieved from https://books.google.com/books/about/Weapons_of_Math_Destruction.html?id=CxD-DAAAQBAJ

Paskarina, C. (2023). Public Trust in the Time of Pandemic: An Analysis of Social Networks in the Discourse of Large-Scale Social Restrictions in Indonesia. Social Sciences 2023, 12(3), 186. https://doi.org/10.3390/SOCSCI12030186

Paskarina, C., Hermawati, R., & Nuraeni. (2021). Politics of Hashtags: Social Network Analysis of Online Contestation in the 2019 Indonesia Presidential Election. Rivista Di Studi Sulla Sostenibilita, (1), 151–170. https://doi.org/10.3280 / RISS2021-001009

Poetranto, I. (2023). Pegasus in Southeast Asia: Civil society targeted with military-grade spyware. Retrieved April 14, 2025, from https://newnaratif.com/pegasus-spyware-in-southeast-asia/

Rouvroy, A., & Berns, T. (2013). Algorithmic Governmentality and Prospects of Emancipation: Disparateness as a precondition for individuation through relationships? Reseaux, (177), 163–196. Retrieved from http://www-01.ibm.com/soft-

Silas, J., Paskarina, C., & Herdiansah, A. G. (2024). Which's more Powerful Digital Power in Papua: Internet Shutdown or Internet Throttling? Journal of Governance, 9(2). Retrieved from https://jurnal.untirta.ac.id/index.php/jog/article/view/24197

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104(July), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Tapsell, R. (2021). Democracy and disinformation in Southeast Asia: The return of digital repression. Pacific Affairs, 94(3), 489–510.

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. BMC Medical Research Methodology, 8(1), 45.

Ufen, A. (2024). The Rise of Digital Repression in Indonesia under Joko Widodo. Retrieved from https://www.giga-hamburg.de/en/publications/giga-focus/the-rise-of-digital-repression-in-indonesia-under-joko-widodo

Ünver, H. A. (2018). Artificial Intelligence, Authoritarianism and the Future of Political Systems. In First Monday. Minnesota, USA: First Monday. https://doi.org/10.5210/fm.v19i7.4901

Wijayanto, W., Setiyono, B., Martini, R., & Elsitra, G. N. (2022, November 16). Digital Authoritarianism in Southeast Asia: A Systematic Literature Review. European Alliance for Innovation. https://doi.org/10.4108/eai.14-9-2021.2321400

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. USA: Public Affairs.