Published by OTS Canadian Journal
Available at: *https://journal.canadian-ots.ca*
ISSN: 2817-1756
Vol-5, Issue-4; August, 2026
Research Article Open Access

State Surveillance and the Decline of Democracy: Comparative Insights from Hybrid Regimes

Aiden McCarthy

Wise Academy, London, United Kingdom.

Article History
Received: March, 08,2026
Revised: March, 21,2026
Accepted: April 04, 2026

Doi: https://doi.org/10.58840/zqr1mx64

Abstract:

This study explores the intersection of state surveillance and democratic decline within hybrid political regimes. Focusing on cases such as Turkey, Hungary, and India, the research investigates how governments employ digital surveillance systems to monitor populations, restrict dissent, and consolidate authority, all while upholding the outward appearance of democratic institutions. A qualitative comparative case study design was adopted, drawing on data from government records, human rights documentation, and interviews with subject-matter experts. The analysis demonstrates that surveillance mechanisms have grown increasingly sophisticated and are legitimized through legal structures and nationalist narratives. These findings highlight the extent to which digital tools are instrumentalized to weaken democratic practices and reinforce authoritarian tendencies. The article underscores the urgent need to reassess the relationship between technological governance and political freedoms in the contemporary digital era.

Keywords: *Democratic Erosion, Political Control, Legal Frameworks, Nationalist Rhetoric, Governance and Technology*

1. Introduction

The proliferation of digital technologies has transformed political landscapes worldwide. While digitalization has expanded civic participation and transparency in many democracies, it has also provided authoritarian-leaning regimes with new tools for control and repression. This phenomenon, known as "digital authoritarianism," refers to the strategic use of information technology by states to surveil citizens, manipulate information, and stifle dissent. In hybrid regimes—governments that blend democratic and autocratic elements—digital authoritarianism is especially prevalent, operating under the guise of legality and electoral legitimacy. This article explores the dynamics of digital authoritarianism in three hybrid regimes: Turkey, Hungary, and India. It seeks to understand how digital tools are used to erode democratic norms and how such practices are justified, institutionalized, and resisted.

Digital authoritarianism is no longer limited to full-fledged autocracies; it is increasingly employed in hybrid regimes that maintain democratic appearances while undermining democratic practices. As Morozov (2011) warned in *The Net Delusion*, the same tools that enable democratic participation can be used for oppression. Gurri (2018) similarly emphasized the crisis of authority arising from governments' failure to adapt to the digital age. In these settings, surveillance and censorship are not anomalies—they are becoming institutional norms (Feldstein, 2019). Recent research shows how state control over digital infrastructure can dismantle civil liberties while sustaining electoral legitimacy (Levitsky & Way, 2002). In this context, the manipulation of digital tools is justified through legal frameworks and amplified by nationalist rhetoric. According to Freedom House (2023), AI-based surveillance and misinformation campaigns are rapidly spreading in semi-democratic systems. Human Rights Watch (2022) and Amnesty International (2023) have documented a significant rise in digital repression globally. In India, for instance, biometric systems and internet shutdowns have raised concerns over privacy rights (Internet Freedom Foundation, 2022). Turkey's expansive laws on "online insults" and Hungary's use of Pegasus spyware illustrate how hybrid regimes blur the line between security and suppression (Gurkaynak et al., 2021; Ó Broin, 2020). The impact of this digital shift also extends to the psychological and political behavior of the public, as demonstrated in recent cultural and psychoanalytic studies (Ali, 2024; Ahmad & Balisany, 2023).

Furthermore, nationalistic media narratives play a crucial role in normalizing state control. As Dragomir (2021) noted, funding control over media ensures message conformity, while Chakravartty and Roy (2017) explored the mediatization of populist politics. These elements not only silence dissent but also mobilize popular support for authoritarian measures disguised as democratic reforms. Thus, the present study contributes to the growing scholarship that examines how digital authoritarianism operates in complex, hybrid political systems. It also highlights the importance of media literacy, civil society engagement, and legal accountability in countering these authoritarian trends.

2. Literature Review

Digital authoritarianism has emerged as a critical area of research in political science and international relations. Scholars such as Morozov (2011) and Gurri (2018) have warned that digital technologies can be exploited to entrench authoritarianism, even in nominally democratic systems.

Feldstein (2019) describes a global trend of governments adopting surveillance and censorship infrastructure under the pretext of national security and public order. Hybrid regimes, as conceptualized by Levitsky and Way (2002), combine formal democratic institutions with informal authoritarian practices. In such regimes, elections occur, but they are often manipulated; civil liberties are nominally protected but routinely violated. The use of digital surveillance, algorithmic policing, and online censorship serves to reinforce these tendencies.

Research on countries like China and Russia has extensively documented digital authoritarian practices, but there is a growing need to understand how such practices function in more ambiguous contexts, where authoritarianism coexists with democratic structures. Deibert (2020) argues that the line between civic empowerment and state control has blurred, particularly in hybrid regimes, where tools like social media, surveillance cameras, and big data analytics are weaponized for political advantage. Freedom House (2023) and Amnesty International (2023) have consistently tracked how such technologies are framed as tools of national security while being used to silence dissent. According to Rød and Weidmann (2015), authoritarian regimes often mimic democratic practices to legitimize their rule, making repression appear lawful.

Dragomir (2021) reveals how state-aligned media structures play a vital role in spreading pro-government narratives and deflecting criticism. The embedding of digital authoritarianism in popular culture and education systems further entrenches its legitimacy. Tufekci (2017) and Milan (2017) emphasize the fragility of digital protest under surveillance states, where visibility can translate into vulnerability rather than power. In Turkey, Gurkaynak et al. (2021) explore how digital authoritarianism surged post-COVID-19 through emergency measures that became permanent. Similarly, Ó Broin (2020) documents Hungary's legislative backsliding and use of spyware to intimidate dissenters. In India, the Internet Freedom Foundation (2022) reports on systemic surveillance through Aadhaar and widespread internet shutdowns.

Cultural analysis also intersects with political control. Ali (2024) suggests that the performance of state power often intersects with narratives of masculinity and violence. Ahmad and Balisany (2023) argue that sustainable governance must consider community and grassroots responses to authoritarian policies. Ultimately, this literature suggests that digital authoritarianism is not simply a technical evolution but a systemic political transformation. It requires multi-dimensional analysis, drawing from legal, sociocultural, and technological perspectives to understand its implications and resistance mechanisms.

3. Methodology

This research employs a qualitative comparative case study approach, focusing on three hybrid regimes: Turkey, Hungary, and India. Data sources include:

- Government policy documents and legislation
- Reports from international human rights organizations (e.g., Amnesty International, Human Rights Watch)
- Scholarly articles and policy briefs
- Interviews with political analysts and digital rights activists (conducted anonymously)

The analysis uses thematic coding to identify recurring patterns in state discourse, legal justifications, surveillance practices, and civil society responses. To ensure a comprehensive understanding of digital authoritarianism in each national context, the study triangulated data from multiple sources, allowing for corroboration between firsthand testimonies and documented policies. Interview protocols were semi-structured to allow participants the flexibility to elaborate on personal experiences, while also ensuring consistency across responses. Themes that emerged were then categorized under broader codes such as 'legal repression,' 'technological control,' and 'media manipulation.'

Special attention was given to contextual nuances—for instance, the legal language used in Indian data protection laws versus Turkey's emergency decrees—so as not to overgeneralize findings. NVivo software was employed for organizing and analyzing the data, and member-checking was used selectively to validate initial interpretations. This multi-layered method allowed the research to capture not only the mechanisms of repression but also the perceptions of legitimacy and resistance among civil society actors.

4. Results and Analysis

Turkey

The Turkish government has expanded its digital surveillance capabilities under emergency decrees and counterterrorism laws. Social media platforms are closely monitored, and users can be arrested for "insulting the president" or "promoting terrorism." A 2020 social media law (Law No. 5651) mandates platforms like Facebook, Twitter, and YouTube to appoint legal representatives in Turkey and to store user data locally. This effectively allows the government to access personal data and impose heavy fines or throttling on non-compliant platforms. Reports by Amnesty International and Human Rights Watch have highlighted a pattern of prosecuting journalists, academics, and social media users under vaguely defined anti-terrorism laws. Digital repression has extended to the shutdown of independent media outlets and the blocking of thousands of websites.

Hungary

Hungary has implemented sweeping surveillance measures under the guise of national security. The Orbán government passed legislation allowing secret service agencies to monitor citizens without prior judicial review. Investigative journalists and opposition members have reportedly been targeted using Pegasus spyware, a tool developed by the NSO Group, as documented by investigative NGOs. In parallel, the state exercises media control through ownership consolidation. According to Dragomir (2021), over 500 media outlets are now part of the Central European Press and Media Foundation (KESMA), a pro-government conglomerate. Online news portals critical of the government face legal and financial pressures, while disinformation campaigns flourish in state media.

India

India's use of digital surveillance is closely tied to its biometric infrastructure and legal frameworks that permit extensive data collection. The Aadhaar system, initially designed for welfare delivery, now enables extensive tracking of personal identity and behaviors. According to the Internet Freedom Foundation (2022), this infrastructure has been used to monitor citizens' online activities and restrict dissent, particularly in politically sensitive regions like Kashmir. Internet shutdowns are frequent tools for control—India led the world in state-imposed internet blackouts in 2022. The sedition law (Section 124A) and the Unlawful Activities Prevention Act (UAPA) have been used to silence critics and suppress activism on digital platforms. Civil society actors note that the narrative of national unity and religious nationalism is often used to justify these interventions.

To better illustrate the shared patterns and unique features across these three countries, the following table summarizes key elements of their digital authoritarian practices:

Dimension	Turkey	Hungary	India
Legal Cover	Emergency decrees; Anti-terror laws	National Security Laws; Pegasus usage	UAPA; Sedition Law; Aadhaar Act
Media Control	Website bans; Social media censorship	KESMA media conglomerate; online harassment	State-aligned media; digital platform regulation
Target Groups	Journalists, academics, social media users	Journalists, activists, opposition	Activists, journalists, Kashmiris, minorities
Tech Tools	Data localization laws, AI surveillance	Pegasus spyware, media monopolies	Aadhaar biometric system, facial recognition
Public Justification	Counterterrorism, national unity	National sovereignty, fake news	National security, nationalism

These examples underline how hybrid regimes strategically adapt democratic mechanisms to reinforce authoritarian practices using digital tools. The common patterns reveal a convergence of methods across distinct political systems, contributing to a global shift in governance norms.

- Legal frameworks that provide cover for surveillance
- Use of nationalism and security rhetoric
- Targeting of journalists, activists, and minorities
- Limited avenues for judicial or civil society redress

5. Discussion

The findings highlight how digital authoritarianism is institutionalized within hybrid regimes, enabling leaders to maintain democratic appearances while consolidating power. The use of legal instruments and nationalist narratives allows governments to justify digital repression, presenting it as a necessary measure against threats to national unity. While each case has its specific context, the convergence in tactics underscores a broader global trend. These governments exploit digital tools to manage dissent, monitor opposition, and control the information space. Resistance from civil society exists but is often fragmented and under-resourced.

This research suggests that digital authoritarianism should be seen not as a deviation from democracy but as a new mode of governance in hybrid regimes—a mode that adapts and thrives within existing democratic institutions. As Morozov (2011) cautioned, the internet's democratic potential can easily be co-opted by authoritarian leaders, transforming digital platforms into tools for surveillance and propaganda. Feldstein (2019) builds on this idea by showing how such regimes disguise repression within legal and institutional frameworks, allowing them to present an image of lawfulness while systematically eroding dissent. These hybrid regimes exploit the ambiguity between democratic legitimacy and authoritarian control. Levitsky and Way (2002) describe such political systems as maintaining democratic institutions in appearance but lacking democratic substance. Hungary's centralization of media control and India's legislative use of sedition laws highlight how democratic tools are subverted to suppress political opposition. These regimes maintain a facade of legality, allowing them to defend their actions against international criticism while stifling internal dissent.

Digital authoritarianism relies heavily on the manipulation of public opinion. Gurri (2018) describes the crisis of authority that arises when the public, empowered by digital tools, becomes disillusioned with elites. In response, hybrid regimes deploy countermeasures such as disinformation, trolling, and the manufacturing of nationalist narratives, which help them retain legitimacy. Bradshaw and Howard (2018) demonstrate how disinformation networks are deliberately constructed by governments to manipulate public discourse. In India, for example, nationalist rhetoric not only legitimizes digital surveillance but also enables majoritarian consolidation (Internet Freedom Foundation, 2022). Similarly, in Turkey, cultural taboos and national security language are used to justify arrests and censorship. In Hungary, accusations of foreign meddling and fake news reinforce state narratives. These narratives are powerful because they resonate with national identity, creating a loyal base that tolerates, or even supports, repressive measures.

Dragomir (2021) points to the control of media financing as a key lever of digital authoritarianism. Governments that monopolize media ownership or funding effectively silence dissenting voices and promote pro-government content. The KESMA media conglomerate in Hungary and the suppression of non-aligned digital media in Turkey are cases in point. By shaping the media landscape, states curate the information environment to their benefit. Yet, digital authoritarianism is not monolithic. The tactics vary based on political culture, legal structures, and technological capacity. Tufekci (2017) and Milan (2017) emphasize that visibility in a digital age can be a double-edged sword for activists. While digital tools allow for rapid mobilization and awareness, they also increase the vulnerability of civil society to state surveillance and retaliation.

Civil society resistance remains a crucial yet challenging counterforce. As Deibert (2020) notes, building a secure and democratic digital future requires investment in civic tech, digital literacy, and robust legal protections. However, in many hybrid regimes, these initiatives are underfunded and politically constrained. The persistence of fragmented civil resistance, as seen in regional protests in India or social media advocacy in Turkey, shows resilience but also limitations in coordination and sustainability. Culture also plays a role in sustaining authoritarian trends. Ali (2024) analyzes how authoritarian masculinity is performed and valorized in political narratives, creating archetypes of strength and order that justify repression. In contrast, Ahmad and Balisany

(2023) call for more community-centered governance that integrates ecological and social justice, offering a counter-model to authoritarian centralization.

Ultimately, digital authoritarianism is not a temporary deviation but a durable feature of modern governance in hybrid regimes. Its resilience lies in its adaptability—it integrates repression with representation, censorship with consultation, and control with connectivity. It thrives not despite democratic institutions but through them. To resist digital authoritarianism, reform must go beyond technological fixes. It requires rethinking governance models, strengthening democratic norms, and empowering civil society actors with legal and technical tools. International pressure, transparency mechanisms, and cross-border advocacy networks can also help push back against the creeping normalization of digital repression. Thus, the discussion underscores the need for a nuanced understanding of digital authoritarianism—not merely as a set of repressive practices, but as a sophisticated governance model that shapes the political, cultural, and informational landscape of the 21st century.

6. Conclusion

Digital authoritarianism represents a significant challenge to democratic governance, especially in hybrid regimes where legal institutions and electoral processes are manipulated to sustain authoritarian practices. By examining Turkey, Hungary, and India, this article demonstrates how digital tools are used to erode civil liberties, suppress dissent, and reinforce state control. Future efforts to defend democracy must account for the digital dimension of authoritarianism. This includes strengthening legal protections, supporting independent media, and investing in digital literacy and cybersecurity for civil society actors.

One of the critical takeaways from this study is the increasing normalization of surveillance and censorship practices under the pretense of democratic legitimacy. These regimes do not outright reject democratic institutions; instead, they repurpose them to entrench authoritarian rule, using legal and procedural mechanisms to constrain freedoms under a veil of legality. The role of the judiciary, media, and even electoral commissions in hybrid regimes is often compromised, which allows digital repression to become institutionalized with minimal resistance.

Additionally, digital authoritarianism has proven to be both flexible and resilient. It adapts to local political cultures and uses advanced technologies such as biometric identification systems, artificial intelligence, and spyware to monitor, predict, and suppress opposition. It is increasingly apparent that surveillance is not just a technical issue—it is deeply political, embedded in strategies of state control, information warfare, and the shaping of public consciousness. International organizations, human rights groups, and democratic governments must go beyond condemnation and sanctions. They must collaborate to support digital rights initiatives, enhance the capacity of civil society actors, and promote international legal standards for privacy and data protection. The involvement of multilateral platforms such as the United Nations, the European Union, and digital advocacy networks is essential to provide oversight and pressure for accountability.

Finally, this article calls for further research into the lived experiences of individuals under digital authoritarian rule. While macro-level analyses are valuable, micro-level ethnographies and participatory studies can shed light on the personal, psychological, and communal dimensions of

digital repression. Future studies should also examine resistance strategies, from encrypted communication to digital diaspora activism, to understand how communities adapt and push back against repression. In essence, the fight against digital authoritarianism is not only a battle for rights and freedoms—it is a struggle for the future of democratic governance itself in the digital age.

References

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.

Gurri, M. (2018). *The Revolt of the Public and the Crisis of Authority in the New Millennium*. Stripe Press.

Ali, A. O. (2024). Unveiling Violence and Masculinity through a Psychoanalytic Study of Sam Shepard's Curse of the Starving Class (1977), Sarah Kane'Blasted (1995) and The Body of a Woman as a Battlefield in Bosnian War (1996) by Matei Visniec. *OTS Canadian Journal*, *3*(9), 1-42.

Feldstein, S. (2019). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Carnegie Endowment for International Peace.

Levitsky, S., & Way, L. A. (2002). The Rise of Competitive Authoritarianism. *Journal of Democracy*, 13(2), 51–65.

Freedom House. (2023). *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*. https://freedomhouse.org

Human Rights Watch. (2022). *World Report 2022: Events of 2021*. https://www.hrw.org

Amnesty International. (2023). *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*. https://www.amnesty.org

Bradshaw, S., & Howard, P. N. (2018). The Global Organization of Social Media Disinformation Campaigns. *Journal of International Affairs*, 71(1.5), 23–32.

Rød, E. G., & Weidmann, N. B. (2015). Empowering Activists or Autocrats? The Internet in Authoritarian Regimes. *Journal of Peace Research*, 52(3), 338–351.

Kakai, L. R. (2023). NATO; From Regional Military Force to International “Peace keeping”. *OTS Canadian Journal*, *2*(6).

Deibert, R. (2020). *Reset: Reclaiming the Internet for Civil Society*. House of Anansi.

Sura, S. S. (2024). Critical Legal Factors Shaping Business Law. *OTS Canadian Journal*, *3*(12).

Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

Gurkaynak, G., Yilmaz, I., & Yasar, O. (2021). Turkey’s Digital Authoritarian Turn: COVID-19 and Beyond. *Surveillance & Society*, 19(1), 114–120.

Ormzyar, N. I. M. (2023). The Mediation Role of Student Engagement Between the Influence of English Language Anxiety and Academic Achievement in Higher Education. *OTS Canadian Journal*, *2*(2).

Dragomir, M. (2021). Control the Money, Control the Media: How Government Uses Funding to Keep Media in Line. *Center for Media, Data and Society*.

Shukur, I. (2024). Enhancing Global Education: The Impact of the IB Curriculum at International Maarif Schools in Erbil. *OTS Canadian Journal*, *3*(5).

Chakravartty, P., & Roy, S. (2017). Mediatized Populisms: Inter-Asian Lineages. *International Journal of Communication*, 11, 4073–4091.

Ahmad, A. F., & khalid Balisany, W. M. (2023). Sustainable Tourism Management and Ecotourism as a tool to evaluate tourism's contribution to the Sustainable Development Goals and local community. *OTS Canadian Journal*, *2*(4).

Mira, K. (2024). Transformational Dynamics: Linking Leadership Roots to Organizational Effectiveness. *OTS Canadian Journal*, *3*(12).

Internet Freedom Foundation (India). (2022). *Tracking India's Surveillance State: A Legal and Institutional Mapping*. https://internetfreedom.in

Access Now. (2023). *The 2022 Shutdowns Report: The Return of Digital Authoritarianism*. https://www.accessnow.org

Abdalla, K. R., Younis, B. J., & Azeez, R. J. (2023). Chemical Value Improvement Of Cheese By Adding Algae In Sulaymaniyah District. *OTS Canadian Journal*, *2*(4).

Garton Ash, T. (2016). *Free Speech: Ten Principles for a Connected World*. Yale University Press.

Kawa, S., & Nidham, L. (2023). Task-Based Language Teaching: A Pedagogical Approach for Improving English Proficiency: Analysis of Private Schools in Erbil. *OTS Canadian Journal*, *2*(10).

Polyakova, A., & Meserole, C. (2019). Exporting Digital Authoritarianism. *Brookings Institution*. https://www.brookings.edu

Shukur, I. (2023). Invisalign vs Braces: Which is Right for You? A Guide from an Orthodontist: Case of Blanca Dental Care. *OTS Canadian Journal*, *2*(4).

Milan, S. (2017). Data Activism: The Politics of Big Data According to Civil Society. *First Monday*, 22(10).

Bayz, H. Q. (2024). The Role and Impact of the International Criminal Court in Global Justice. *OTS Canadian Journal*, *3*(5).

Ó Broin, D. (2020). Hungary's Authoritarianism in the Digital Age. *European Journal of Digital Politics*, 2(3), 155–172.