

AI in Non-Free and Autocratizing Contexts: Trends, Theoretical Frameworks, and the Minimum Digital Security Package

Andrej Kallaur¹

¹ Masaryk University, Brno, Czechia; ORCID: <https://orcid.org/0000-0002-6010-2557>

Email: kallaur@mail.muni.cz

ROR <https://ror.org/02i46qs45>

Abstract. Drawing on a systematic synthesis of academic literature and reports from leading research institutions, this article conceptualizes contemporary trends in AI deployment within non-democratic regimes. I argue that while AI empowers autocrats and helps establish a baseline toolkit to deter regime transition, digital capabilities alone remain insufficient without traditional hard power. Nevertheless, global technological diffusion and cross-border collaboration within the “authoritarian international” facilitate a *minimum digital security package*. This mechanism enables less technologically advanced non-democracies to mitigate risks through AI-driven surveillance, censorship, and information manipulation.

Keywords: AI; digital authoritarianism; censorship; communication; surveillance

Introduction

On May 27, 2026, the *Financial Times* published the article “China Overhauls World’s Biggest Surveillance Network with Advanced AI”. Its China Technology Correspondent, Eleanor Olcott, managed to interview industry insiders, including an executive from Hikvision – the Chinese video surveillance manufacturer and supplier blacklisted by the U.S. Commerce Department due to human rights violations and its cameras’ usage associated with China’s mass incarceration of Uyghurs (Bhuiyan, 2022). Revealing local government procurement tenders across Chinese provinces, she shows how local authorities pursue Beijing’s drive toward so-called “predictive policing” by overhauling their surveillance network with advanced AI. What is actually changing with AI enhancement? According to the article, local governments receive the unprecedented capacity to monitor behavior at scale. Now, AI allows them to “interpret scenes, identify patterns of behavior, and retrieve footage using written prompts” (Olcott, 2026). One of the explicit examples provided in the text is that “Hikvision’s latest products enable operators to search footage using prompts such as ‘a woman wearing a red hat’ and automatically retrieve relevant video” (Olcott, 2026).

In the analytical and academic literature on the rise of digital authoritarianism, there is a heavy bias toward the study of China and Russia. As political scientist Ildar Daminov highlights (2025, p. 409), “More research on other cases of covert repression is necessary.” Existing literature focuses heavily on how hegemonic powers like Russia and China develop, apply, and export hardware and software for digital repression. For example, Polyakova and Meserole (2019), in their policy brief “Exporting digital authoritarianism: The Russian and Chinese models” for the Brookings Institution, analyzed their strategic division of labor between Moscow and Beijing: “While China is driving innovation in high-tech social control, Russia has been more willing to weaponize information technologies as part of targeted influence operations.” In a recent study on Russian digital authoritarianism published by MIT Press, Bronnikova et al. (2025) acknowledged that “Belarusian trainers are important actors in the security training ecosystem within the post-Soviet space, due to the scale of repression in the country and the know-how they have

Received: 2026-10-03. Accepted: 2026-10-10.

therefore acquired” (2025, p. 94). However, even as researchers recognize the significance of non-hegemonic powers, scholarship on how these authoritarian regimes digitalize remains in its infancy, especially in light of the rapid accessibility of the AI revolution. Although a growing body of literature has begun to examine digital authoritarianism in cases such as Belarus (Avdieieva et al., 2022; Rudnik, 2024; Korshunau, 2026), Syria, and several Southeast Asian states (Gohdes, 2020; Gerard, 2022), these empirical insights remain fragmented. Furthermore, the impact of AI on digital authoritarianism remains underexplored, as academic analysis of its long-term trajectories is only beginning to emerge (see, for instance, Anastasopoulos & Lian, 2026; Gunitsky & Schneier, 2026). Among the causes of this digital rise, researchers usually cite pre-established infrastructure, institutional uncertainty, and the structural politico-economic context (Gohdes, 2020; Korshunau, 2026; Daminov, 2025). I emphasize that an overlooked and broader factor is rapid technological development and the AI revolution. Increasingly, state-led digitalization extends beyond resource-rich authoritarian powers like China and Russia to encompass capacity-limited non-democratic regimes

AI Regulation across Regimes: The Free vs. Not and Partly Free Divide

The character of AI debates – most relevant in the digital field due to the ongoing AI revolution (Institute for Policy Research, 2025) – differs significantly between the Free and Not and Partly Free countries, distinctions defined by Freedom House that I apply here, which should be taken into account for the contextual division of current legal and international affairs. In this framework, a “Free” country achieves high overall scores, indicating greater freedom; “Partly Free” denotes partial respect for political rights and civil liberties, whereas a “Not Free” country receives the lowest combined scores, representing the smallest degree of freedom regarding electoral processes, political pluralism, government functioning, expression, and individual rights (Freedom House, n.d.).

For instance, “the European Union has led the charge on strong regulation, prioritizing ‘trustworthy AI,’ which must be lawful, ethical, and robust. China’s AI policies, while outwardly similar, diverge in practice on key issues like personal privacy” (Institute for Policy Research, 2025). In 2024, EU lawmakers adopted the AI Act, making the EU the first jurisdiction with such a comprehensive legal framework for AI. Chapter II, Article 5 of the regulation outlines prohibited AI practices, including the “placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques” as well as the use of “‘real-time’ remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement,” subject to specific exceptions (European Parliament & Council of the European Union, 2024). In 2023, seven Chinese government agencies jointly approved and issued the *Interim Measures for the Management of Generative Artificial Intelligence Services*. Article 4 of the regulation stipulates that the provision and use of generative AI services must uphold Core Socialist Values and refrain from generating content prohibited by law, such as material that incites the subversion of state power or the overthrow of the socialist system (Cyberspace Administration of China, 2023). In Russia, artificial intelligence development is guided by a formal national strategy, updated under Presidential Decree №124 of February 15, 2024. According to the document, key priorities include technological sovereignty – defined as ensuring the necessary level of independence for the Russian Federation in the field of artificial intelligence (Ukaz Prezidenta RF №124, 2024). More broadly, regulatory frameworks for AI in non-democracies remain in their formative stages. In fact, this holds true even for powers like China and Russia, neither of which has established a comprehensive framework equivalent to the EU AI Act. It remains uncertain what trajectory their regulatory models will follow, particularly given that formal legal boundaries often play a secondary role to political and state imperatives in non-democratic regimes. While discussions within the European Union focus on the technological implications for public and private rights, and deregulation aims to encourage innovation in the US (patchwork approach), the context, as we see, shifts when looking at non-democratic regimes.

Today, AI is making a serious push in the development of digital suppression technologies. Much like in the free world, where AI analyzes large amounts of data and creates new content, non-democracies also embrace facial recognition technology and generative AI. Without evident public control and freedom and rights protections, these tools lead to greater organizational strengths of power, making these regimes more stable in terms of survival. How AI develops, where and how it is applied, differs significantly between Free and Not and Partly Free countries. In this conceptual paper, I synthesize two primary streams of literature to map how contemporary scholarship examines AI deployment in non-free and autocratizing contexts: peer-reviewed academic studies

identified via targeted Google Scholar queries on digital authoritarianism, alongside analytical reports from leading global institutions (such as Freedom House and the Brookings Institution). Building on these insights, I introduce the concept of the *minimum digital security package* to explain how less technologically advanced non-democracies leverage cross-border technology transfers to mitigate regime threats.

AI Revolution & AI Sovereignty

The symbol of today's AI scaling is data centers worldwide – the final destinations of a microchip supply chain that has triggered hardware shortages and immense demands for electricity. To generate vast amounts of energy, mega-scale installations such as the Colossus supercomputer rely on gas turbines. Operating an AI data center requires an integrated ecosystem comprising high-density compute clusters, high-speed networking, specialized liquid cooling, resilient power infrastructure, and specialized machine learning operations software platform. The ultimate output of this infrastructure is the training, fine-tuning, and deployment of frontier artificial intelligence models – powering generative AI applications, multimodal systems, and autonomous agents at scale. According to Brynjolfsson et al. (2023), the rapid pace of generative AI development occurred due to the convergence of four core factors: first, computational scale; second, innovations in model architecture; third, the ability to pre-train using massive amounts of data; and fourth, refinements in training techniques. Beraja et al. (2023) highlight AI technology as the foundation of a “fourth industrial revolution” that will power long-term economic growth.

OpenAI researchers Kokotajlo et al. (2025) predict an even more profound acceleration in AI capabilities by 2027, outlining a scenario in which model alignment and goal setting become increasingly opaque:

The researchers don't have the ability to directly set the goals of any of their AIs. Indeed, the researchers think that the concept of 'true goals' is probably a massive oversimplification, but they don't have a better theory to replace it with, much less one that has been thoroughly vetted. They disagree internally about whether the AIs are trying to follow human instructions, or seeking reinforcement, or something else, and they can't just check.

Driven by the AI race between the United States and China – despite export controls and restrictions limiting China's access to advanced microchips, with rare exceptions like NVIDIA's H200 AI chip (Hawkins, 2026) – states and corporations increasingly pursue *AI sovereignty*. Autocrats are developing their own infrastructure, collaborating with one another, and promoting their domestic technologies within an “authoritarian international” (Silitiski, 2010; Hall, 2023), competing directly with the free world. In this context, Vitali Silitiski (2010) defines the “authoritarian international” as a collaborative alignment among non-democratic regimes aimed at collectively defending themselves against external democracy promotion and regime-change pressures. For instance, Belarus and Russia developed the *SKIF* supercomputer, which state-aligned media praised as an “achievement in high-performance computing that can rightfully be called a symbol of technological sovereignty and a historic breakthrough” (Ob'edinennyi institut problem informatiki Natsional'noi akademii nauk Belarusi, 2026).

According to Beraja et al. (2023, p. 2), trade patterns in surveillance technology reveal a distinct political orientation in technology transfers:

Autocracies and weak democracies are more likely to import facial recognition AI from China. For example, we observe that 45% of China's export deals are with autocracies and weak democracies, while only 23% of US exports are with those countries. These patterns are particularly striking given the generally higher income and higher trade volumes of (strong) democratic regimes. Such political bias is not seen in US exports of AI or China's exports of other frontier technologies.

In this sense, artificial intelligence has become both a catalyst for cooperation and a new arena for the deepening cleavage between democracies and non-democracies.

What constitutes sovereign AI? Ustun (2026) defines the concept through the lens of comprehensive technological autonomy:

[Sovereignty] is either a country's or an organization's capacity to independently develop, deploy, and govern artificial intelligence using its own infrastructure, its own data, its own models, and its own talent. It is not about owning the technology. It's about retaining full control over the entire AI life cycle – from the physical compute to the algorithmic logic.

As part of the AI race, governments and companies pursue the goal of achieving AGI (artificial general intelligence), which refers to a hypothetical AI that can match or exceed human intelligence across any intellectual task, rather than just specialized ones. Chan (2026) observes a distinct pragmatic shift in Chinese technological strategy:

While some Chinese AI companies, such as DeepSeek and Alibaba, also talk about trying to achieve AGI, Chinese policymakers and China's AI industry as a whole are more focused on running several different AI races. They are more focused on making progress in model efficiency, AI adoption, and the integration of AI into the physical world.

According to Chan (2026), robotics and so-called “embodied AI” are a key priority for Chinese policymakers. He warns us that “as AI systems grow more powerful, so does their potential for misuse. From AI-enhanced cyberattacks to deepfakes to AI-enabled bioweapons, both the scope and scale of potential malicious uses of AI are expanding.” Nevertheless, such technological sovereignty is not confined to individual states or corporations but extends across broader geopolitical alignments between democratic and non-democratic regimes. The Eurasian Economic Union and the Shanghai Cooperation Organization are examples of such alignments. This dynamic is reflected not only in Russia's national strategy on AI, but also in strategic policy frameworks in the West. For instance, the policy document *Winning the Race: America's AI Action Plan*, published by the Trump administration, explicitly sets the competitive tone in its opening line, declaring that “[t]he United States is in a race to achieve global dominance in artificial intelligence (AI)” (The White House, 2025).

The Minimum Digital Security Package

In the following chapter and subchapters, I examine the primary AI-enhanced tools explicitly traded, deployed, and refined within Not Free and Partly Free countries, identified through a synthesis of academic literature and expert analytical reports. The concept of the minimum digital security package explains how less technologically advanced non-democracies leverage cross-border technology transfers to mitigate regimes risks. Empirical evidence from academic studies and reporting reveals that non-democratic regimes increasingly develop, train on, and commercialize these security tools collectively. As AI advances, these tools become increasingly accessible even in the face of international export controls and sanctions. Consequently, less technologically advanced regimes acquire a baseline technological shield against domestic uprisings. Simultaneously, autocratic hegemonies expand their sphere of technological alignment and influence, while smaller non-democratic states actively participate in technology exchanges, often serving as critical nodes in supply chains. Based on empirical findings, this minimum digital security package fundamentally consists of three core components: AI-driven surveillance, automated censorship, and targeted information manipulation.

AI Facial Recognition in Surveillance

The most comprehensive AI surveillance architecture was first deployed in China to target and control the Uyghur minority in Xinjiang. However, today this system has become AI-enhanced, has expanded across all Chinese provinces, and is subsequently exported globally. As Gerard (2022) reports, countries such as Myanmar, Cambodia, Thailand, Indonesia, and the Philippines receive technical support and surveillance technologies from China and Russia. Beyond software and hardware delivery, China also conducts training in surveillance methodologies, hosting diplomats from Myanmar, Laos, and Vietnam at a specialized academy in Guangxi (Gerard, 2022).

Broadly defined, AI-powered surveillance “utilizes machine learning algorithms with vast amounts of data from everyday activities, allowing public authorities and companies to monitor, track, analyze, and identify human behaviors in real-time and at scale” (Choung et al., 2024). In democratic contexts, critics highlight severe privacy risks, potential infringements on civil liberties, unauthorized data collection, lack of consent, and function creep (Choung et al., 2024). Conversely, in non-democratic regimes, “security imperatives” routine override civil liberties entirely.

Driven by recent breakthroughs in generative AI and computer vision, these systems have advanced significantly. Olcott (2026) notes that modern Chinese networks “are trained to predict and issue alerts for behaviors including erratic driving, crowd build-ups, unauthorized entry, and suicidal behavior.” Furthermore, major vendor updates, such as Hikvision's latest product suite, integrate large language models (LLMs) that allow operators to perform

natural-language video queries (e.g., searching for “a woman wearing a red hat”) to immediately retrieve targeted footage (Olcott, 2026).

Beyond major global powers, locally developed automated surveillance networks are also operational within smaller, non-hegemonic autocracies. In Belarus, for example, state-aligned automated monitoring has been active since 2017. According to Belarusian authorities, approximately 60,000 cameras currently run the Kipod AI facial recognition platform, developed by the Belarusian firm Synesis (Dev.by, 2024). Kipod leverages cloud-based big data and computer vision to identify individuals, track vehicles, map movement, and automatically flag security incidents across the country. Mirroring their Chinese counterparts, domestic firms such as Synesis specialize in developing AI systems to reinforce state control across other post-Soviet authoritarian regimes, including Kazakhstan and Azerbaijan, where the Kipod platform facilitates real-time tracking and public surveillance in high-density areas (CityDog.io, 2018).

Generative AI and Censorship

It might seem that AI chat censorship is nothing new, acting merely as an extension of the censorship already seen on traditional media platforms – for instance, the TikTok channels of Belarusian opposition figures like Tsikhanouskaya and Latushka have been blocked by the Chinese platform in Belarus (Naša Niva, 2025).

The digital landscape in autocracies like Belarus, as in many other non-democracies, is significantly reshaped by the rapid rise of the Chinese neural network DeepSeek. By offering a chatbot without subscription fees, DeepSeek lowered financial and technical barriers to entry, with its highest adoption rate recorded in China (89%), followed by Russia, Iran, Cuba, and Belarus at 56% (Microsoft 2026). In Belarus, ChatGPT, Claude, Gemini, and Grok are unavailable, as their developers have restricted access to the country (Euroradio 2026).

Martens (2025) notes that DeepSeek also characterizes a new approach in the AI race where access to advanced microchips is limited:

The arrival of DeepSeek marks the start of a new cycle in AI model development. Models build on top of each other, with recursive development between models to accelerate AI learning at ever lower cost. The approach to model training based on training-data collection, pre-training and fine-tuning by a single firm is being replaced by a more horizontal networked model, potentially reshaping the AI field by proliferation and interaction – some call it free-riding – between AI models, combining distillation of knowledge and distributed training across models (Moussa et al. 2025). AI systems are being pulled out of a small number of big compute silos and sucked into a universe of smaller, more-powerful models with lower end-user inference costs.

The Center for AI Standards and Innovation (CAISI) at the Department of Commerce’s National Institute of Standards and Technology (NIST) evaluated AI models from the People’s Republic of China (PRC) developer DeepSeek and found that they lag behind U.S. models in performance, cost, security, and adoption; however, DeepSeek models echoed four times as many inaccurate and misleading Chinese Communist Party narratives as U.S. reference models did (NIST, 2025). This systemic alignment with state ideology is further illustrated by qualitative prompting tests. For instance, when presented with queries regarding political repression in China, DeepSeek issues a standardized refusal: *“Sorry, that’s beyond my current scope. Let’s talk about something else.”* As Euroradio (2026) observes, when asked about political persecution in Belarus, DeepSeek framed its response around official state narratives, stating that “Minsk denies its existence,” outlining international assessments, and reiterating that “the Belarusian authorities categorically reject” such claims. Similarly, Yandex’s AI assistant “Alisa” evades contemporary political sensitivities entirely: when queried about human rights violations in Belarus, the chatbot restricts its response to historical events in the Soviet era (the Belarusian SSR), completely omitting modern political realities (Euroradio, 2026).

AI-Enhanced Pro-Regime Communication

Funk et al. (2023) observed that “AI-based tools that can generate text, audio, and imagery have quickly grown more sophisticated, accessible, and easy to use, spurring a concerning escalation of these disinformation tactics,” noting that generative technologies were deployed in at least 16 countries to influence public debate.

The most prominent application of AI in political communication is the deployment of deepfakes by pro-authoritarian actors. For instance, an explicit usage of deepfakes with direct impact occurred when a video “appeared to show Ukraine’s president, Volodymyr Zelensky, telling his people to surrender” a few weeks into the full-scale Russian invasion (Clark & Lewandowsky, 2026). However, even when deepfakes exhibit low visual quality or logical inconsistencies, audiences do not automatically reject them – a finding empirical research confirms (Clark & Lewandowsky, 2026). In their study, Clark and Lewandowsky (2026) demonstrated that:

Participants exposed to a specific warning were substantially more likely to recognize the video as a deepfake, whereas a generic warning – alerting participants to the general existence of deepfakes – had no measurable effect on their belief regarding the video’s authenticity.

Conceptually, Villasenor (2019) defines deepfakes as videos “that have been constructed to make a person appear to say or do something that they never said or did,” while Lyu (2024) broadly characterizes deepfakes as “any digital media created or edited by generative AI algorithms.” These synthetic artifacts serve to “discredit or intimidate people, influence political opinion and elections, and undermine our criminal justice system by creating doubt about the reliability of video evidence in general, even when it is not fake” (Clark & Lewandowsky, 2026).

Deepfake deployment is increasingly widespread globally. Beacken et al. (2026) examined computational propaganda in non-free and autocratizing contexts – specifically Bolivia, Hungary, India, Nigeria, Tunisia, and Turkey – “where distinctions between authoritarian and democratic propaganda are progressively blurring.” According to the authors, generative AI scales and transforms digital propaganda by automating the creation of persuasive, hard-to-detect multimodal content – including deepfake video, voice clones, and synthetic text – while enabling real-time micro-targeting and rapid translation across minority dialects. They categorized their cases into “Explorers” (Bolivia, Hungary, Tunisia, and Turkey), where generative AI propaganda remains anticipated or in its early stages, and “Experimentalists” (India and Nigeria), where political elites actively deploy advanced generative AI tools, such as voice clones of deceased or prominent figures, dialect-tailored translations, synthetic endorsement videos, and plausible deniability strategies. A critical finding from Beacken et al. (2026) that aligns with this study is that non-democracies operate within globally interconnected propaganda networks:

Across contexts, interviewees compared their countries with others they considered similar, drawing on shared histories, regional ties, and power relations. This reflects conceptualizations of contemporary propaganda as globally interconnected (Wasserman & Madrid-Morales, 2022) and shaped by history, culture, and power (Kuo & Marwick, 2021).

In Belarus, supporters of the Lukashenka regime leverage deepfakes to produce fabricated videos and deploy automated bot networks for mass comment attacks against critical online content. A prominent example involved a widely circulated deepfake targeting opposition leader Sviatlana Tsikhanouskaya, which falsely depicted her resigning from political leadership (Zerkalo.io, 2025). Furthermore, this AI toolkit is emerging as an exportable dimension of authoritarian collaboration. In its bilateral relations with Myanmar, Belarus has expanded ties beyond traditional military-technical cooperation to incorporate IT-driven military media and AI-assisted content generation (CTV, 2025). During an official delegation visit to the Belarusian military broadcaster *VoyenTV*, state media highlighted that foreign representatives specifically inspected AI-generated video products, illustrating a growing convergence between military production and automated information control (CTV, 2025).

Future Trajectories and Theoretical Boundaries

As demonstrated, AI does not create an entirely new political realm; rather, it is embedded within established mechanisms of control and manipulation, such as state surveillance, censorship, and propaganda. Current literature struggles to provide overarching theoretical frameworks beyond traditional definitions of digital authoritarianism and repression. Feldstein (2021) conceptualized digital repression as the use of information and communication technology to surveil, coerce, or manipulate individuals or groups to deter activities that challenge the state. While visible physical violence aimed at quelling mass unrest can undermine state legitimacy, digital strategies lower the risk of escalating violence while maintaining political control (Feldstein, 2021).

Another theoretical framework that could align with AI-driven non-democracies is surveillance capitalism (Zuboff, 2019). Because AI requires vast datasets for training and real-time analysis, data collection has become vital not only for tech conglomerates but also for autocracies and their corporate partners. As Zuboff defines it, surveillance capitalism represents “the unilateral claiming of private human experience as free raw material for translation

into behavioral data,” which are then processed to construct prediction products (Laidler, 2019). In non-free and autocratizing contexts, the logic of market surveillance overlaps with digital state control: both systems rely on behavioral data extraction and predictive modeling – with non-democracies leveraging these tools to prevent regime threats. Driven by existential regime insecurity, they pursue rapid technological transformations. As Brynjolfsson and McAfee (2014) observed regarding technological development, “steady exponential improvement has brought us into the second half of the chessboard – into a time when what’s come before is no longer a particularly reliable guide to what will happen next.” Consequently, while AI may not yet alter the fundamental essence of non-democracies today, its medium-term trajectory remains highly unpredictable. What is evident is that AI technologies create opportunities for cross-border trade, learning and tech diffusion within “authoritarian international,” deepening the cleavage between free and unfree worlds. Furthermore, developments like DeepSeek demonstrate that autocracies can build capable AI systems even under strict microchip export controls. By removing the need for massive human surveillance bureaucracies, the *Minimum Digital Security Package* provides non-hegemonic non-democracies with a baseline toolkit to stabilize power and prevent mass unrest.

However, AI exhibits clear structural vulnerabilities and should not be viewed as an infallible mechanism of total control. Anastasopoulos and Lian (2026) highlight systemic failure modes, such as misidentification and missed threats: “a neighbor misidentified by facial recognition, a benign post flagged by filters, or routine movement misread as suspicious... are not mere statistical annoyances.” Crucially, when algorithms are tuned to reduce noise, genuine political threats can slip through, allowing opposition networks to coordinate in ways unseen by the model. Furthermore, because AI models are trained on historical data, they assume past patterns will predict future threats – yet under active state surveillance, opposition tactics and “ground truth” constantly evolve (Anastasopoulos & Lian, 2026). Ultimately, many contemporary autocracies survive “not through technological control but through extreme violence... In each case, AI pushed resistance to adapt but did not quell it” (Anastasopoulos & Lian, 2026).

Finally, future research should look beyond global superpowers to examine how autocracies adopt, adapt, and trade the Minimum Digital Security Package, as well as what the growing autonomy and capacity for independent action of agentic and embodied AI may mean for the future of digital authoritarianism (Stryker n.d.).

AI use

AI tools, specifically Gemini Pro, were used for language improvement and proofreading.

Disclosure statement

The author reports no conflict of interest.

References

- Anastasopoulos, L. J., & Lian, J. (2026). The limits of authoritarian AI. *Journal of Democracy*, 37(2), 5–17. <https://doi.org/10.1353/jod.2026.a986016>
- Avdieieva, T., Krapiva, N., Okremova, D., Zhymont, A., & Ziniakova, T. (2022). *Digital dictatorship: Authoritarian tactics and resistance in Eastern Europe and Central Asia*. Access Now. <https://issuelab.org/permalink/resource/42459>
- Beacken, G. D., Trauthig, I. K., & Woolley, S. C. (2026). Generative AI, propaganda, and digital authoritarianism: Comparative insights from six democratically weakened countries. *Big Data & Society*, 13(2). <https://doi.org/10.1177/20539517251410064>
- Beraja, M., Kao, A., Yang, D., & Yuchtman, N. (2023). *Exporting the surveillance state via trade in AI* (Working Paper). National Bureau of Economic Research. <https://doi.org/10.3386/w31676>
- Bhuiyan, J. (2022, December 29). Police in China can track protests by enabling ‘alarms’ on Hikvision software. *The Guardian*. <https://www.theguardian.com/world/2022/dec/29/china-surveillance-protests-alarms-cameras-hikvision>

- Bronnikova, O., Ermoshina, K., & Zaytseva, A. (2025). Digital security training: GAFAM/MAGMA, data protection, and encryption. In F. Daucé, B. Loveluck, & F. Musiani (Eds.), *Digital authoritarianism in the making: Repression and resistance on the Russian internet* (pp. 93–116). The MIT Press. <https://doi.org/10.7551/mitpress/15798.003.0009>
- Brynjolfsson, E., Li, D., & Raymond, L. R. (2023). *Generative AI at work* (Working Paper No. 31161). National Bureau of Economic Research. <https://doi.org/10.3386/w31161>
- Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.
- Chan, K. (2026, April 16). *Competing AI strategies for the US and China*. Brookings Institution. <https://www.brookings.edu/articles/competing-ai-strategies-for-the-us-and-china/>
- Choung, H., David, P., & Ling, T.-W. (2024). Acceptance of AI-powered facial recognition technology in surveillance scenarios: Role of trust, security, and privacy perceptions. *Technology in Society*, 79, Article 102721. <https://doi.org/10.1016/j.techsoc.2024.102721>
- CityDog.io. (2018, May 18). *Posmotrite, kak za vami nablyudayut s videokamer na ulitsakh Minska* [Look at how you are being monitored by street video cameras in Minsk]. <https://citydog.io/post/zaden-kamery-minsk/>
- Clark, S., & Lewandowsky, S. (2026). The continued influence of AI-generated deepfake videos despite transparency warnings. *Communications Psychology*, 4(1), Article 13. <https://doi.org/10.1038/s44271-025-00381-9>
- CTV. (2025, October 23). *Voennye Belarusi i Myanmy obsudili voprosy vzaimodeystviya v informatsionnoy sfere* [Belarusian and Myanmar military discussed issues of interaction in the information sphere]. <https://ctv.by/news/obshchestvo/voennye-belarusi-i-myanmar-obsudili-voprosy-vzaimodeystviya-v-informacionnoj-sfere>
- Cyberspace Administration of China. (2023). *Interim measures for the management of generative artificial intelligence services*. Australian National University. <http://hdl.handle.net/1885/295663>
- Daminov, I. (2025). When do authoritarian regimes use digital technologies for covert repression? A qualitative comparative analysis (QCA) of politico-economic conditions. *Swiss Political Science Review*, 31, 406–434. <https://doi.org/10.1111/spsr.12607>
- Dev.by. (2024, March 5). *Za belarusami sledyat 35 tysyach kamer. V 2021 godu bylo 700* [Belarusians are being watched by 35,000 cameras. In 2021 there were 700]. <https://devby.io/news/za-belarusami-sledyat-35-tysyach-kamer-v-2021-godu-bylo-700-1709550122>
- Euroradio. (2026, July 6). *ChatGPT is unavailable in Belarus. Russian and Chinese AI are filling the gap*. <https://euroradio.fm/en/chatgpt-claude-and-gemini-are-unavailable-belarus-what-are-offered-instead>
- European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689
- Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.
- Freedom House. (n.d.). *Freedom in the World research methodology*. <https://freedomhouse.org/reports/freedom-world/freedom-world-research-methodology>

- Funk, A., Shahbaz, A., & Vesteinsson, K. (2023, October). *Freedom on the Net 2023: The repressive power of artificial intelligence*. Freedom House. <https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence>
- Gerard, M. (2022, September). From the editor: The spectre of digital authoritarianism for Southeast Asia. *Kyoto Review of Southeast Asia*, 33. <https://kyotoreview.org/issue-33/from-the-editor-the-spectre-of-digital-authoritarianism-for-southeast-asia/>
- Gohdes, A. (2020). Repression technology: Internet accessibility and state violence. *American Journal of Political Science*, 64(3), 488–503. <https://doi.org/10.1111/ajps.12509>
- Gunitsky, S., & Schneier, B. (2026, October 1). The AI autocrat: How technology empowers—and imperils—dictators. *Foreign Affairs*. <https://www.foreignaffairs.com/united-states/artificial-intelligence-autocrat-technology-empowers-dictators>
- Hall, S. (2023). *The authoritarian international: Tracing how authoritarian regimes learn in the post-Soviet space*. Cambridge University Press.
- Hawkins, A. (2026, September 29). Lawmakers plan to cut off China from AI chips. Nvidia, AMD want Trump to intervene. *Politico*. <https://www.politico.com/news/2026/09/29/nvidia-amd-trump-chips-china-ai-01096445>
- Institute for Policy Research. (2025, March 27). *The AI revolution: Hype, reality, and what comes next*. Northwestern University. <https://www.ipr.northwestern.edu/news/2025/the-ai-revolution.html>
- Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. AI Futures Project. <https://ai-2027.com/>
- Korshunau, H. (2026). Political regime transformations: Digital authoritarianism, repression, and the internet. In A. Kazharski (Ed.), *Routledge handbook of contemporary Belarus* (pp. 77–88). Routledge.
- Laidler, J. (2019, March 4). High tech is watching you. *The Harvard Gazette*. <https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>
- Lyu, S. (2024). DeepFake the menace: Mitigating the negative impacts of AI-generated content. *Organizational Cybersecurity Journal: Practice, Process & People*, 4(1), 1–18. <https://doi.org/10.1108/OCJ-08-2022-0014>
- Martens, B. (2025). *How DeepSeek has changed artificial intelligence and what it means for Europe* (Policy Brief No. 12/2025). Bruegel. <https://www.bruegel.org/policy-brief/how-deepseek-has-changed-artificial-intelligence-and-what-it-means-europe>
- Microsoft. (2026). *Global AI adoption in 2025: A widening digital divide*. <https://www.microsoft.com/en-us/research/wp-content/uploads/2026/01/Microsoft-AI-Diffusion-Report-2025-H2.pdf>
- Naša Niva. (2025). *Na terytorii Bielarusi zablakavali tyktok-kanaly Cichanoŭskaj i Łatuški* [TikTok channels of Tsikhanouskaya and Latushka blocked in Belarus]. <https://nashaniva.com/369922>
- National Institute of Standards and Technology. (2025). *CAISI evaluation of DeepSeek AI models finds shortcomings and risks*. <https://www.nist.gov/news-events/news/2025/09/caisi-evaluation-deepseek-ai-models-finds-shortcomings-and-risks>
- Ob’edinennyi institut problem informatiki Natsional’noi akademii nauk Belarusi. (2026, April 6). *Superkomp’yutery “SKIF” — tekhnologicheskij proryv Soyuznogo gosudarstva* [“SKIF” supercomputers — A technological breakthrough of the Union State]. <https://uiip.by/rus/news/657/>
- Olcott, E. (2026, May 27). China overhauls world’s biggest surveillance network with advanced AI. *Financial Times*. <https://www.ft.com/content/f8fa4739-4359-4720-af77-9be1e8370f82>

- Polyakova, A., & Meserole, C. (2019, August 27). *Exporting digital authoritarianism: The Russian and Chinese models*. Brookings Institution. <https://www.brookings.edu/articles/exporting-digital-authoritarianism-the-russian-and-chinese-models/>
- Rudnik, A. (2024). Co-option of technology: Digital repression and legitimization strategies of the Belarusian regime. *Communist and Post-Communist Studies*, 57(4), 28–55. <https://doi.org/10.1525/cpcs.2024.2125064>
- Silitski, V. (2010). "Survival of the fittest": Development of authoritarianism in Belarus. *Communist and Post-Communist Studies*, 43(4), 339–350. <https://doi.org/10.1016/j.postcomstud.2010.10.007>
- Stryker, C. (n.d.). *What is agentic AI?* IBM. <https://www.ibm.com/think/topics/agentic-ai>
- Ukaz Prezidenta RF No. 124 (2024, February 15). "O vnesenii izmenenii v Ukaz Prezidenta Rossiiskoi Federatsii ot 10 oktyabrya 2019 g. No. 490 'O razvitii iskusstvennogo intellekta v Rossiiskoi Federatsii' i v Natsional'nuyu strategiyu, utverzhdenuyu etim Ukazom" [Decree of the President of the Russian Federation of February 15, 2024 No. 124 "On Amendments to Decree of the President of the Russian Federation of October 10, 2019 No. 490 'On the Development of Artificial Intelligence in the Russian Federation' and to the National Strategy Approved by This Decree"]. (2024, February 15). *Ofitsial'nyi internet-portal pravovoi informatsii* (No. 0001202402150063). <http://publication.pravo.gov.ru/document/0001202402150063>
- Ustun, A., Bennici, L., & Krawina, M. (2026, March 6). *What is sovereign AI?* McKinsey & Company. <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-sovereign-ai>
- Villasenor, J. (2019, February 14). *Artificial intelligence, deepfakes, and the uncertain future of truth*. Brookings Institution. <https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/>
- The White House. (2025, July). *Winning the race: America's AI action plan*. Executive Office of the President. <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>
- Zerkalo.io. (2025, January 12). *V internete rasprostranili dipfeyk s Tikhanovskoy* [A deepfake featuring Tsikhanouskaya has been circulated online]. <https://news.zerkalo.io/economics/89477.html>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs

Author biography: Andrej Kallaur holds a PhD in Political Science with a specialization in Security and Strategic Studies from Masaryk University. He balances corporate and academic roles, working as an Enablement Lead and AI Research Lead Fellow while serving as a Visiting Lecturer. His research interests lie at the intersection of technology, politics, and communication.