Diffusion of Digital Authoritarianism? Censorship, Surveillance, and Beyond in Türkiye

Mesut Aslan[1] and Gözde Yilmaz[2]

Abstract

The expansion of authoritarianism in the world has led to increased debates about digital authoritarianism as well as the diffusion of authoritarianism. However, these two topics have not been addressed together despite the digital world being a strong candidate for diffusion. This study explores whether digital authoritarian diffusion occurs from China and/or Russia to Türkiye by examining the models of China and Russia and unpacking the Turkish model of digital authoritarianism. We argue that the Turkish model is inspired by the Chinese and Russian models, but without the active promotion of those models by authoritarian centers. Instead, analyses of the legal framework, technology, and surveillance practices suggest that there is an indirect and passive as well as internally driven process at work.

Keywords: Authoritarianism, Diffusion, Digital Authoritarianism, Digital Surveillance, Internet Sovereignty

[1] Department of International Relations, AHBV University, Ankara, Türkiye, aslan.mesut@hbv.edu.tr https://orcid.org/0000-0003-0299-0928

[2] Department of International Relations, Atilim University, Ankara, Türkiye, gozde.yilmaz@atilim.edu.tr https://orcid.org/0000-0003-3015-568X

Introduction

Authoritarianism has been on the rise around the world in recent decades. An "authoritarian resurgence" or a "third wave of authoritarianism" reflects the proliferation of authoritarian systems in the world and the erosion of democratic systems (Brownlee, 2017; Lührmann & Lindberg, 2019). While the expansion of authoritarian systems has been a reality, digital authoritarianism and its diffusion have become particularly important issues with the expansion of new technological improvements.

Digital authoritarianism as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations," is the new game among authoritarian regimes (Polyakova & Meserole, 2019, p. 1). Tools for digital authoritarianism are commonly used in many autocratic systems and the digital growth of Chinese and Russian power has led to debates about the diffusion of the Chinese and Russian models in the digital sphere. Diffusion in the digital sphere is most likely since the rate of interaction in that realm is high and it can easily lead to learning, copying, or emulation. Digital authoritarian diffusion could be driven by the usual suspects, namely Russia and China, by providing models for learning or promoting autocracy directly.

China and Russia represent the "sovereign and controlled internet governance model" in contrast to the "open model supported by many liberal democracies" (Sherman 2021, p.110) and, therefore, provide models for authoritarian states to adopt digital authoritarianism. Rather than favoring the free flow of information through the internet, Russian and Chinese models focus on online censorship and surveillance worldwide and emerge as models for the diffusion of digital authoritarianism (Bradford, 2023, p. 46; Polyakova & Meserole, 2019, p. 1; Shahbaz, 2018, p. 1; Sinkkonen & Lassila, 2020, pp. 3–4). Due to its great power status while keeping its draconian stance in the digital sphere, China, and due to its continuous impact and low-cost methods, Russia are both considered models for digital authoritarianism. China's internet sovereignty discourse and its globally notable national technology scene, combined with similar technical and regulatory approaches, make China a prominent case for digital authoritarianism. Moreover, governments within Russia's sphere of influence "have been early adopters of more subtle, temporary, legal, or plausibly deniable forms of "next generation" controls, increasing use of surveillance, proregime content production, behind the-scenes pressures, and court cases or legal justifications to alter the online informational environment" (Kerr, 2018, p. 3828).

In this study, we analyze digital authoritarianism from two perspectives. First, we explore the control and manipulation of information in the digital sphere by comparing internet

governance models. Normative approaches and various domestic legal regulations of the regimes of interest provide a strengthening harmony within both authoritarian and democratic governance models in the digital sphere. Second, we address surveillance assemblages that interconnect the physical and digital spheres while utilizing various tools and methods in tandem to consolidate power and repress or deter opposition and dissent. Since governments utilize "surveillance, cyberattacks, and disinformation to consolidate their power and expand it beyond borders" (Michaelsen & Glasius, 2018, p. 3788) we categorize these activities under control and manipulation of information and surveillance.

The case of Türkiye is vital for understanding the possible influence of authoritarian powers in the digital sphere as it has demonstrated a rising competitive authoritarian regime since 2010 (Esen & Gumuscu, 2016) and the increasing use and control of digital resources to manage opponents. As in every corner of the world, digital surveillance, internet censorship, and dis/misinformation are all being increasingly applied in Türkiye for the survival and consolidation of the authoritarian regime.

Considering the aforementioned probability of diffusion in the digital area, this study aims to determine whether there is digital authoritarian diffusion from China and/or Russia to Türkiye by examining the models of China and Russia and unpacking the Turkish model of digital authoritarianism. It is argued here that the Turkish system of digital authoritarianism has been inspired by both the Chinese and Russian models. However, it is not possible to identify an active diffusion mechanism from those authoritarian gravity centers to other authoritarian regimes. Rather, there is an indirect and passive as well as internally driven process at work.
This research is an exploratory case study that aims to identify diffusion of digital authoritarianism from China and/or Russia by unpacking the case of Türkiye. The article explores, first, the Chinese and Russian model of digital authoritarianism and, second, it compares these models with the Turkish model of digital authoritarianism. Such exploratory research is necessary before examining the mechanisms of diffusion such as learning, or emulation and this article provides a preliminary analysis for this purpose. The article aims to show some degree of diffusion of digital authoritarianism from China and Russia towards Türkiye. Demonstrated by the Turkish case. This paves the way for future research that needs to focus on the mechanisms of diffusion and trace the process.

The next section of this article focuses on digital authoritarianism and diffusion processes. The second part explores the Russian and Chinese models of digital authoritarianism while the fourth unpacks digital authoritarianism in Türkiye and positions Türkiye's approach

to the digital sphere by focusing on surveillance, internet censorship, dis/misinformation, and various other policies. The final section provides the concluding remarks.

A New Game in Town: Digital Authoritarianism and Its Diffusion

Digital authoritarianism, as the authoritarian states usage of the digital technology for repression, surveillance and manipulation emerge as the usage of new technologies has become a tool for both insurgency in authoritarian regimes and repression by authoritarian centers (Polyakova & Meserole, 2019, p. 2). While digital advancements empower the repressed in the face of existing regimes by providing alternative means for revolution, such as social media, repressors have also gained new tools for surveillance and manipulation. Advances in technology have provided new resources for authoritarian regimes to control the masses via censoring, surveillance, misinformation, and disinformation. In short, digital authoritarianism is "a way for governments to control their citizens through technology" (Shahbaz, 2018, p. 2) and it "facilitates power consolidation" (Sherman, 2021, p. 108). This is done through "innovative new technologies, such as artificial intelligence and a facial recognition technology these days" (Lee, 2022, p. 22).

The digital sphere, particularly with the growing prevalence of the internet, was seen as a new space that would support democracy and democratization, where freedom of expression would thrive and government interventions would be impractical, unwarranted, and unwanted (Allison, 2002, p. 4; Barlow, 1996; Jiang, 2010, p. 71; Kedzie, 1997, pp. 6–8). Simply, the digital sphere was considered "radically liberal in nature" (Mueller, 2010, p. 5). However, the prevalence of the internet in authoritarian regimes quickly deflated these views of the inescapable freedom of the internet, especially with high-profile cases such as that between Google and the Chinese Communist Party (CCP) in 2010 (Jiang, 2010, pp. 71–72).

Digital authoritarianism includes diverse techniques such as "internet censorship; online harassment; cyber-attacks; internet shutdowns; targeted persecution against online users" and many others (Jamil, 2021, p. 9). Both China and Russia support the "sovereign and controlled internet governance model" rather than the "open model supported by many liberal democracies" (Sherman, 2021, p. 110). They are, therefore, both opposed to the free flow of information through the internet and favor online censorship and surveillance in the wider global arena.

The rise of digital authoritarianism and its diffusion poses several challenges to the world including its expansion within authoritarian states; its expansion abroad, even for surveilling the citizens of other countries; its exportation to like-minded regimes; and the

adoption of digital authoritarian tools by democratic countries (Yayboke & Brannen, 2020, p. 2). Therefore, one of the main challenges posed by digital authoritarianism is authoritarian diffusion, which is suggested to be underway in many countries in different forms via exportation by authoritarian powers and particularly China and Russia (Yayboke & Brannen, 2020, p. 5). For instance, Vietnam adopted a cybersecurity law that is quite similar to the Chinese law; Uganda and Tanzania adopted similarly restrictive laws; Malaysia adopted a facial recognition system within its army; Ecuador implemented surveillance systems that are similar to those of China; Zimbabwe and Angola signed partnerships with a Chinese company, ZTE, to implement artificial intelligence systems; and Huawei introduced smart/safe city systems in more than 100 countries (Matheson, 2020, p. 5; Polyakova & Meserole, 2019, p. 6; Shahbaz, 2018, p. 8; Sherman, 2021, p. 110).

Authoritarian diffusion, or "the process by which institutions, organizations, policies, strategies, rhetorical frames, norms, etc. which establish, protect, or strengthen authoritarian rule, are reproduced from one authoritarian system to another" (Ambrosio & Tolstrup, 2019, p. 2744), is being increasingly explored within the literature (e.g., Ambrosio, 2010; Brownlee, 2017; Kneuer & Demmelhuber, 2016; Tansey, 2016; Tolstrup, 2015). However, there is a need for detailed case studies focusing on authoritarian diffusion in different contexts to confirm the existence of authoritarian diffusion, because initiatives such as these could merely be the cooperation of two authoritarian states in the digital sphere rather than signifying authoritarian diffusion.

The travel of authoritarian norms and policies from one authoritarian system to another could be either externally or internally driven (Ambrosio & Tolstrup, 2019, p. 2744). In externally driven processes, external actors are "instrumental in causing other actors to adopt a particular item" (Ambrosio & Tolstrup, 2019, p. 2744). Therefore, there could be an active influence of an authoritarian power through autocracy sponsorship and more coercive techniques (Tansey, 2016, p. 153). In addition, the question of whether the main motivation behind the autocratic sponsorship is ideological or not brings us to the respective consequences of autocracy promotion with an ideological motivation or simply resistance to democracy in the case of no specific ideological baggage (Tansey, 2016, p. 153). Autocracy promotion could be an external attempt from the authoritarian center to prevent democrats from becoming dominant in the target country or region, but it could also provide models for emulation, copying, or learning, which brings us to internally driven authoritarian diffusion (Kneuer & Demmelhuber, 2016, p. 777).

Internally driven diffusion or voluntary forms of diffusion entail actors learning from other authoritarians in a process that involves the search for a solution abroad to a particular problem at home (Ambrosio & Tolstrup, 2019, p. 2746). For the survival of the regime, it is necessary to seek "examples of other authoritarian successes or failures and [apply] those lessons to their current or expected political situation" (Hall & Ambrosio, 2017, p. 144). In drawing lessons from other authoritarians, it becomes easier for these actors to develop "a collection of policies and institutional changes to make them better able to resist democratic pressures at home and from abroad" (Ambrosio, 2018, p. 121). In such processes, the model that the lessons are drawn from is vital for the learning, and authoritarian states might drive authoritarian diffusion simply by serving as models rather than by actively promoting autocracy. In that case, passive influence from the authoritarian center is at work. Authoritarian diffusion may also emerge voluntarily via emulation as "a process whereby policies spread because they are socially valued independently of the functions they perform." (Meseguer & Gilardi, 2009, p. 530). Therefore, unlike learning, in this form of diffusion there is no relevance of the consequences or success of a policy. Instead, "the symbolic and socially constructed characteristics of policies are crucial" (Maggetti & Gilardi, 2016, p. 5). Emulation involves policies that "conform to their normative environment" and, therefore, some policies are accepted "regardless of whether they 'work' or not" and some others "will be taboo, even though they could possibly be beneficial" (Gilardi, 2016, p. 10). Furthermore, competition, as another form of internally driven or voluntary diffusion, is an additional process whereby actors may "react to one another in an attempt to attract or retain resources" (Maggetti & Gilardi, 2016, p. 5). Competition can take political, economic, and social forms.

Most importantly, many scholars (e.g., Brownlee, 2017; Casier, 2022; Risse & Babayan, 2015; Way, 2015; Weyland, 2017; Yilmaz & Eliküçük Yıldırım, 2020) have concluded that there is no such thing as active and intentional sponsorship of authoritarianism pushed by authoritarian centers. While we might discuss unintentional authoritarian diffusion within the authoritarian toolbox, with authoritarian models taken for learning, the literature nevertheless holds that there is no autocracy promotion from the authoritarian centers of China or Russia (e.g., Yakouchyk, 2019, p. 156). Rather, it seems that cooperation among authoritarian actors may empower authoritarian regimes without the intentional sponsorship of autocracy (Risse & Babayan, 2015, p. 384). As Yılmaz and Eliküçük (2020) emphasized, there may be "unintentional consequences" of authoritarian cooperation rather than autocracy sponsorship. As a result, actors may strengthen a regime through cooperation in different areas and unintentionally promote autocracy.

Because of the debate within the literature on the existence of authoritarian diffusion, there is a need for further case studies to explore authoritarian diffusion from authoritarian centers. The digital realm is conveniently available for diffusion even in remote territories, but researchers still need to look beyond the traditional means of authoritarianism and expand their scope to digital authoritarianism. First and foremost, there is a need to unpack the models of diffusion of digital authoritarianism, which will be explored in the next section.

Russian and Chinese Models for Diffusion of Digital Authoritarianism

The digital sphere has created a new space where political actors, private firms, and the public actively and increasingly participate on a daily basis. This global information flow necessitates new and distinct governance approaches towards the digital sphere (Mueller, 2010, pp. 1–2). The Russian and Chinese models constitute important attempts to govern the digital sphere in this regard. These cases were selected here because both governments provide insights into authoritarian diffusion in the digital world. In particular, the internet sovereignty argument of China, which receives support from Russia, provides "political cover" for other regimes and actors are more likely to adopt norms and practices that are contrary to dominant trends when political cover is provided. On the other hand, regimes that are working to strengthen their own power turn to the models that seem most likely to allow them to meet their goals. Finally, as relatively strong and stable authoritarian regimes in the global system, Russia and China constitute general models for like-minded regimes, which includes influence in the digital sphere (Ambrosio, 2010, p. 382). In this sense, we argue that the cases of Russia and China both have merit from the perspective of authoritarian diffusion, which enables us to show that these models are available for potential adopters as the converging goals of both regimes are somewhat achieved and they provide some level of normative political cover for digital authoritarianism. We will now summarize the current approaches of these so-called authoritarian centers, which will subsequently enable us to position the Turkish model relative to these two models.

The only comprehensive official document detailing China's internet sovereignty is a whitepaper published by the Information Office of the State Council in 2010 (Shen, 2016, p. 90). Succinctly, internet sovereignty considers the digital sphere as an extension of the physical world under the control of a sovereign within its physical borders, in contrast to the Western view of the internet as a new interconnected and transnational space exempt from any single government's control. The whitepaper states the following: "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China

should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security." It also acknowledges the difference of governance between states by stating: "National situations and cultural traditions differ among countries, and so concern about Internet security also differs" (*The Internet in China*, 2010). Thus, China has created an isolated alternative digital sphere that functions as an extension of the country's physical world. This, in turn, creates a heavily controlled area not unlike traditional news and media agencies.

The Chinese model for digital authoritarianism has been carefully crafted in recent decades by engaging with the digital sphere directly via different policies such as building the Great Firewall of China. The Great Firewall "surveils, intercepts, and blocks internet transmissions according to the requirements of the CCP" (Qiang, 2021, p. 35). We also see that the Chinese model relies on "censorship, propaganda and AI-driven population-wide surveillance" (Qiang, 2021, p. 35). Most importantly, new technologies like facial recognition systems are used extensively in Chinese digital authoritarianism. China has been trying to surveil its citizens by linking the internet with the physical world, as done by the social credit system launched in 2020 to measure the trustworthiness of citizens with both online and offline data (Polyakova and Meserole, 2019, p. 4). China increasingly uses artificial intelligence for "facial recognition, identifying persons and patterns of interest through predictive policing and automating content moderation" (Peterson, 2020, p. 5).

Examples of high-tech surveillance include Skynet, which envisages surveillance of the masses via the creation of a network of CCTVs and the quick and easy identification of people, or Sharp Eyes, providing surveillance in rural areas through the installation of cameras in possible "crowd-gathering places in rural areas" (Qiang, 2021, p. 36). Chinese tech companies are also developing smart/safe city platforms, incorporating "data analytics and automated security into a city's infrastructure in an effort to digitally detect crime, manage city traffic and improve municipal efficiency" (Matheson, 2020, p. 5). China has thus become the "supplier of choice for illiberal regimes looking to deploy surveillance systems of their own" (Polyakova and Meserole, 2019, p. 2). It is the main provider of infrastructure development to many countries such as Egypt and Türkiye through its Digital Silk Road Initiative under the auspices of the Belt and Road Initiative and the application of systems like smart/safe cities (Qiang, 2021, p. 38; Shahbaz, 2018, p. 8). This proves that such policies do not remain within a country's borders; they may transcend those borders and even diffuse to remote territories.

Russia is one of the few states that openly supports China's internet sovereignty approach (Budnitsky & Jia, 2018, p. 4). However, Russia's governance model is rather different than that of the CCP. The Chinese model relies on state-of-the-art filtering systems to control or prevent the spread of information in the digital sphere, while the Russian model relies on the spread of mis/disinformation and intimidation (Morgus, 2022, pp. 89–90). There are two main reasons for these differences. First, when Russia initially encountered the global internet, the government did not take the necessary "precautions" to control the flow of information in the digital sphere. Compared to China, this resulted in stronger economic, technical, and social ties with the global internet in Russia, resulting in a more interconnected society (Polyakova & Meserole, 2019, p. 6). The second reason, which is partly due to the first, is that Russia lacks the necessary know-how and economic strength to create its own national tech giants, social media platforms, economic power and general infrastructure, or alternatives to the global digital sphere, which Russian businesses and society rely on. While Russia does offer some alternative national services and platforms, they are not as successful as their Chinese counterparts. For instance, Baidu, Yandex, and Alphabet offer services somewhat similar to those of Chinese or American companies, such as search functions, email, and maps. In other areas, however, Russia does not have feasible alternatives to the giants of the US and China, such as Alibaba, Amazon, Huawei, and ZTE. Even the US is struggling to create communication infrastructure alternatives to Huawei (Janofsky, 2020). In summary, Russia does not have strong alternatives to Western services and platforms because the country does not enjoy the advantages of China in terms of population, market cap, and technological infrastructure. This is one of the main reasons why Russia cannot directly block access to Western services with a blanket ban and strictly control national services, as China does, without serious economic and social backslash. However, Russia securitizes the digital sphere for regime survival and argues for internet sovereignty (Nocetti, 2015, pp. 113, 116). Thus, Russia has had to create a different model, which is more attractive to authoritarian regimes that do not possess China's capabilities (Morgus, 2022, p. 89).

The Russian model includes various techniques to control and govern the digital sphere in tandem. First, the government controls national services through strict laws and coercion. One popular example is the story of the founder of VKontakte (VK), Pavel Durov. VK is one of the biggest social media companies in Russia. However, in 2014 Durov left the company, stating that he was pushed out because he did not comply with the government's request for information about users involved in protests in Ukraine (Toor, 2014). Durov claimed that VK was now under the control of government allies, and he fled Russia. In 2021, that company was

taken over by the Gazprom and Sogaz groups, which are closely linked to Putin and his allies (Marrow, 2021b). Durov went on to found Telegram, one of the most popular privacy-focused online messaging services. In 2018, Russia banned the service after Durov refused to provide user data to the government. However, due to various techniques utilized by users and by Telegram itself, the ban was not very effective. In 2020, the government halted its efforts to block the platform as the cat-and-mouse games between Telegram and the government were affecting legitimate services such as Google, Amazon, and payment services that businesses relied on, as well as general digital entertainment and social platforms. The case of this ineffective ban supports our conceptualization of the Russian model. Russia did not have the technological capacity to isolate and ban specific Telegram traffic and could not afford a general ban since the collateral damage impacted other global services while national services were not available or were not on par with the blocked ones (Ermoshina & Musiani, 2021). In the end, the government changed its tactics and employed contractors to place advertisements or incentive messages on certain Telegram channels to spread propaganda and pro-government discourse via the platform (*Как Telegram-Каналы Стали Инструментом Власти*, 2018).

The Russian system relies on more of a "combination of self-censorship and intimidation underpinned by complex, but ultimately highly restrictive, speech and expression laws and pervasive overt telecommunications surveillance" (Morgus, 2019, p. 89). Therefore, it makes use of "deterrence provided by punishment and physical control over the offline space rather than on comprehensive digital surveillance" (Sinkkonen & Lassila, 2020, p. 4). Most importantly, the Russian model differs from the Chinese with its reliance on repressive laws and on "information manipulation" based on pro-government propaganda (Morgus, 2019, p. 90). Importantly, Russia "has a more decentralized internet infrastructure than China, and is therefore relatively more dependent on legislation than on technical capabilities in controlling content" (Flonk, 2021, p. 1933).

Russia's reliance on deterrence and repression instead of surveillance could be attributed to the differences between the regimes' structures. While both the Chinese and the Russian government view the digital sphere and the flow of information as threats to their rule, for Russia the threat vectors are different from those of China. Since the CCP has a stronger grasp on power compared to the populist rule of Russia, the CCP tends to be more proactive in this area. While both states securitize issues in the digital sphere and they have similar aims and goals (Flonk, 2021), the Russian government is more vulnerable to popular dissent compared to China. Due to these differences, Russia is more focused on the control of information while

China is working towards creating a more comprehensive and integrated environment between the digital and the physical world.

Importantly, the high-tech Chinese model is not the only one ready for diffusion. The low-tech alternative Russian model appeals to countries that do not have the infrastructure required to apply the Chinese model. As Polyakova and Meserole (2019, p. 7) emphasized, the Russian model could be "more adaptable globally as emerging authoritarian regimes that cannot afford China's high-tech model seek greater control over domestic populations and influence abroad." Affordances are also a limitation for most of the "rising" authoritarian regimes as China is able to rely on its gargantuan lucrative market created by the 1.4 billion citizens living under its rule. This economic power is different from capital investment and almost impossible to imitate successfully in other countries. Such a unique advantage gives the Chinese government the ability to block most foreign platforms or services and cultivate its local alternatives. These alternatives have strong ties to the CCP and are subject to the government's wishes and control. One of the many examples of this strategy is the globally popular social media platform TikTok. Developed by the Chinese ByteDance corporation, TikTok is banned in China. Instead, ByteDance has an alternative platform called Douyin available in the Chinese market. "Douyin features restrictions such as blocks on international content and limits on children's usage. The Chinese state owns a stake in the [ByteDance] subsidiary that controls its domestic Chinese social media and information platforms" (Barry, 2022).

While Russia normatively follows the Chinese model, practical limitations push the government to pursue a more creative and versatile strategy. National companies are largely controlled by allies of the government or are bound by strict laws, providing critical information to the government. This, in turn, creates self-censorship among users of the national digital services and platforms. Global services are sometimes banned, but lately the government tries to pressure foreign companies to store Russian users' data and open offices within Russian territory. Throttling the connections and applying fines for failing to remove content in a timely manner are also prevalent methods (Marrow, 2021a; Reuters, 2021a, 2021b, 2021c). This dual approach creates a relatively controlled environment for the authoritarian regime. Since the Russian model does not heavily rely on technological capacity or highly successful national tech giants, it is more accessible for other authoritarian regimes.

Türkiye's approach has some similarities to both the Chinese and Russian models. However, once again due to practical requirements, the Turkish model also has significant differences, which are mostly facilitated by Western tech giants' fear of missing out. To unpack this, the Turkish model will be explored next.

Digital Authoritarianism in Türkiye: Censorship, Surveillance, and Beyond

Compared to China, where national services and platforms are thriving and Western services are banned, and to Russia, where national alternatives are somewhat feasible, the digital landscape of Türkiye does not have meaningful national alternatives to digital platforms and Turkish citizens largely depend on Western services such as WhatsApp, Instagram, X (Twitter), and Facebook. Accordingly, Türkiye's internet governance model has significant differences due to technical and market limitations. However, the government's general approach to control and surveillance follows the models of China and Russia, particularly regarding domestic politics in the digital sphere.

Freedom of speech in general and freedom of the internet by extension is not one of the contemporary Turkish government's strong suits (Çetinkaya & Güngördü, 2021). Freedom House listed Türkiye as "partly free" in 2017 and since then Türkiye has been considered "not free" in the categories of global freedoms and internet freedoms by that group (Turkey: Freedom in the World 2022, 2022). Since 2002, under the strong grasp of the Justice and Development Party (AKP: *Adalet ve Kalkınma Partisi*), the governance of the internet has gone through significant changes. Today, Freedom House reports on Türkiye, China and Russia present similar findings between these countries, especially on the freedom of speech. Number of repressed or detained journalists are on the rise due to vaguely worded laws, state regulators control the traditional media, and censorship, detainments and disinformation campaigns by the government are continue to be prevalent in the digital world in all three countries (China: Freedom in the World 2023 Country Report, 2024; Russia: Freedom in the World 2023 Country Report, 2024; Turkey: Freedom in the World 2023 Country Report, 2024).

The move towards the control of the information on the internet began in 2007, when the government passed a law creating a legal framework to block access to websites related to categorical crimes such as "incitement to suicide, facilitation of the use of narcotics, child pornography, obscenity, prostitution, facilitation of gambling, and slandering of the legacy of Ataturk (the founder of modern Turkey)" (Yesil et al., 2017, p. 5). Since the government does not provide detailed statistics, independent monitoring groups try to collect information about the censorship of websites in Türkiye. One independent report stated that more than 460,000 websites are currently blocked in Türkiye. However, the same report showed that after 2018 there was a steep decline in the number of blocked websites. In 2018, 94,000 websites were blocked by various government institutions, compared to 61,000 in 2019 and 58,000 in 2020 (Akdeniz & Güven, 2020, pp. 1–4). We argue that there are two main reasons behind this decline, which show the evolution of Türkiye's internet governance model. First, the digital

sphere has become increasingly centralized around social media (Derakhshan, 2015; Holmes, 2013). This results in people relying on social media channels instead of traditional independent websites and this consolidation has resulted in a shift in the government's focus. Second, the Turkish government aims to control the flow of information instead of blocking it, similarly to the Russian model. Since most of the interactions, dissent, and general information flow are now taking place on social media platforms, blocking access to relatively unknown websites started to lose its importance apart from a few widely popular platforms such as news outlets. Furthermore, blocking websites results in both domestic and international pressure. Due to the global evolution of the digital sphere, with this reliance on and popularity of global social media platforms in Turkish society, blocking access to services and platforms is now an ineffective strategy with major domestic and international political costs. It appears that the government tends to throttle traffic or regionally block access for a limited time during "crises" instead of issuing complete bans (Bulman, 2016; Wong, 2016). This refined approach, instead of total blocks, gained legal standing when the government amended the 2007 law in 2020.

New laws show that Türkiye is focused on more efficient and less obtrusive methods to avoid international and domestic pressure while expanding government control in the digital world. Türkiye's approach to digital governance puts it in a precarious place. The state supports the multi-stakeholder governance approach of the West on international issues, but in domestic politics regulations show that the government adopts the internet sovereignty approach (Eldem, 2020, p. 11). Under the 2020 regulations, social network providers with more than ten million daily requests from Türkiye must take swift action as requested by government agencies and courts, respond to individual requests, appoint national official representation within the borders of the country, and provide "any and all documents" to authorities that are required for the implementation of the regulations ("Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts", 2022). Failure to comply with the new regulations is punishable by a tiered system, which starts with fines and could result in the throttling of access by up to 90%. Popular services also need to store Turkish users' data in Türkiye (Akdeniz, 2022). These regulations are argued to be aimed at the protection of Turkish citizens in the digital world by taking precautions against hate speech, disinformation, and criminal activity. However, "it would be naive to believe that the Internet Law and its recent amendments aim to tackle 'only' hate speech and illegal content on social networks" (Coşkun, 2021, p. 10). Due to the numerous recent regulations and amendments, intelligence agencies can now request information about users without a court order (Eldem, 2020, p. 8). This, in turn, shows that the "protecting user rights" discourse is borrowed from the West, but in practice

these regulations follow the information control policies of China and Russia (Eldem, 2020, p. 9). For example, Türkiye's practical approach resembles the Russian model with its fines, throttling, and local data storage. Since these regulations are defended as necessary for the privacy and security of citizens and follow global democratic norms with similarity to regulations in Germany, France, and the US (Sarı, 2020), Türkiye has some political cover for its regulations. On the other hand, the effectiveness of the Russian policies provides an easy way for Türkiye to mimic authoritarian practices in the digital world. The discourse of safeguarding the personal data of citizens from corporations and utilizing surveillance for security purposes seems to be relatively effective since the CCP implements its authoritarian regulations while hiding behind global regulations such as the EU's General Data Protection Regulation for cover (Qin et al., 2022). However, the CCP's approach created an unexpected result as "China and the European Union are moving forward with establishing data regimes that have more in common with each other than with that of the United States" (Sacks, 2018). Of course, the legal frameworks of the EU and the CCP differ on key issues since the Chinese model is generally "about securing the Party-State control over cyberspace" (Burnay, 2019, p. 13). Similarly, the Turkish regulations are found to be "intrusive" and "problematic" and "should be either abolished or revised" (Clayton et al., 2016, pp. 6–7). While liberal democracies – albeit not without their own issues and debates – pass regulations to protect the privacy of their citizens, stifle hate speech, and fight crime in the digital sphere, these regulations enable authoritarian governments such as Türkiye to follow in China's footsteps and create draconian regulations under the cover of the same discourse.

The history of surveillance in Türkiye is most comparable to that of Russia as both regimes strengthened and expanded their control after critical events such as mass protests or war efforts (Ünver, 2018, pp. 94–95). Reports show that today all internet service providers in Türkiye are required to submit hourly updates to the Information and Communication Technologies Authority (ICTA). These updates include identifiable network traffic information on all internet users (Eroğlu, 2022a, 2022b). According to experts, the unprecedented scope and amount of collected information give the ICTA both individual profiling and mass surveillance capabilities. Since there are no official documents explaining the goal of this government database or who has access to it (Eroğlu, 2022c), these practices seem similar to the Russian System of Operative Investigative Measures (SORM), which is an "Orwellian network that jeopardizes privacy and the ability to use telecommunications to oppose the government" (Soldatov & Borogan, 2013, p. 23) by forcing service providers to install required software and hardware in their systems to provide government agencies such as the Federal Security Service

unsupervised access to data (Lokot, 2018, p. 338). SORM's working principles are parallel to Türkiye's regulations, as Türkiye is also known to utilize various digital surveillance methods including "deep packet inspection and mass digital surveillance platforms, such as the Phorm, PackageShaper, Remote Control Systems, Hacking Team, FinFisher, and Procera Networks" (Ünver, 2018, p. 95), reflecting technical similarities to the Chinese model. These technical similarities are also in line with the legal frameworks because the solutions are very similar to those of Russia and China. For example China also legally requires ISPs to record identifiable data about their users (Deibert, 2008, p. 265). While it is not possible to clarify whether these technologies are imported directly or recreated by the Turkish authorities, in principle the end result shows that effective solutions of authoritarian centers are implemented at both policy and technical levels.

The lack of clarity in the latest regulations and general criminal law as well as the traditional freedom of expression performance of Türkiye make these regulations "another advanced censorship tool to protect to government's own interest" (Akdeniz, 2022) instead of protecting users or limiting disinformation and propaganda in the digital sphere. Reviewing the legal fine print or comparing Turkish regulations with liberal counterparts strengthens this argument, and analyzing the practical implications and applications clarifies the government's approach, which is geared towards strengthening control and censorship from the perspective of regime security. In the end, Türkiye's priorities in its internet policy situate the state closer to the Russia-China axis in global internet governance debates (Eldem, 2020, p. 10).

The compliance of social media platforms with the new regulations shows that these services are willing to "put profit above the protection of their users" (Clarke, 2021). The first company that appointed a national representative to Türkiye was VK in November 2020, while Western services such as Facebook, YouTube, and Twitter did not comply within the specified legal timeframe and were fined by the government. After numerous fines, YouTube announced in December 2020 that it would comply with the new regulations, and this was closely followed by other platforms announcing their compliance in January 2021 (Akdeniz, 2022). The sequence of these announcements is important because it shows that social media platforms waited for someone to take the first step: in this case, YouTube. In the end, these companies were able to point to both the hefty fines and other services' compliance in efforts to avoid criticism or pressure from the West. Furthermore, the possibility of traffic throttling, which is practically the same as blocking access, means that the Turkish digital market could potentially have become dominated by other services such as VK or Yandex due to their willingness to cooperate with the regime.

Today the general trend among Western platforms is to obey national regulations in fear of missing out to national alternatives or being forced to exit the market and lose significant revenue. Examples such as TikTok, which will be storing US users' data on Oracle's servers after pressure from the US government (Wang & Shepardson, 2022), provide a strong argument for both the compliance of social media platforms and authoritarian governments' requests. While the government is able to control the flow of information in the digital sphere through these strategies, surveillance practices are also a strong indicator of digital authoritarianism in Türkiye. Western providers try to avoid receiving bans or irritating the Turkish government because the Chinese and Russian examples show that alternative models could practically prevent them from competing in the market or result in significant revenue loss. While social media platforms have met with criticism, they claim that they are respecting and protecting their users' voices and data in Türkiye (Akyol, 2021). However, they are silent on details about how to achieve their promises in practical terms, which seems infeasible under current regulations and laws (Akdeniz, 2021; Çetinkaya & Güngördü, 2021), and reports show that even legitimate journalists and critics can be detained under these regulations (Turkey: Freedom in the World 2023 Country Report, 2024).

Türkiye is the leading country in requesting content removals on Twitter and Reddit (Çetinkaya & Güngördü, 2021). Similar to website blocking, the Turkish government does not provide statistics about such requests or their contexts, which further abstracts the proportion of requests that constitute limitations on free speech versus a fight against digital crimes, abuse, or issues such as hate speech and misinformation. Due to the lack of official statistics, most of the research on this subject cites social media companies' transparency reports. However, that approach is fundamentally flawed in the case of Twitter, as the company states that the reports are not comprehensive or complete. Researchers analyzing Türkiye's government requests found "two orders of magnitude more censorship than Twitter officially reports" and the "vast bulk of censored tweets contained political content" (Tanash et al., 2015, pp. 11–19). While Twitter admits to its incomplete reporting (Twitter, 2022), the scale of discrepancy suggests that efforts to ease the tension between the Turkish government and the company by complying with regulations fully to avoid a complete ban play a significant role here. It should also be noted that this is not a new strategy; for example, in 2014, "negotiations were afoot so Türkiye could keep Twitter around, and Twitter could accommodate Turkey's censorship needs" (Tanash et al., 2015, p. 14). It seems that the government and Twitter were able to create a somewhat working relationship protecting both sides' interests as, in recent years, Twitter has not been blocked in any meaningful way by the government.

While most research to date has focused on Twitter, other platforms are following the same path and jeopardizing online free speech and the privacy of Turkish users under the new regulations (Çetinkaya & Güngördü, 2021). The legal representative of YouTube and Twitter in Türkiye stated the following to the Parliament's Committee on Digital Outlets: "As you can imagine, when such legislation is passed at a time when there was hesitation from the viewpoint of international firms such as 'Who will do what, should we be the first to do it or not, what will the effects be?' we think Google's stance by taking such a step [to appoint a representative] on January 12, 2021, set an example in terms of efforts to comply with the legislation…" (Kenez, 2022).

Türkiye does not possess the comprehensive capabilities of China or Russia; however, independent reports show that relatively high-tech strategies are utilized both domestically and in some neighboring areas. Nation-state spyware concealed as legitimate software was installed on users' computers in Hatay, Gaziantep, Adana, Diyarbakir, the Ulus district of Ankara, and in some Syrian regions that were using the Türk Telekom infrastructure with Sandvine PacketLogic devices (Marczak et al., 2018, pp. 20–21). While the operational knowledge, staff, and hardware for these operations were provided by Western companies, similar "in-path network injection" techniques were also used by China's Great Cannon in 2015 and 2017. A deep packet inspection method used for blocking websites and digital surveillance is also utilized by the Great Firewall of China (Brewster, 2016; Marczak et al., 2018, pp. 8–34). The technical similarities support our proof-of-concept argument that inspiration provided by China could be effective in Türkiye in this context. The utilization of private companies for surveillance and control in the digital world is part of "a related, emerging problem" (Zittrain & Palfrey, 2008, p. 31). Although China successfully exports its innovative authoritarian tools (Feldstein, 2019, p. 8), the lack of available relevant information from Türkiye prevents us from pinpointing active efforts to export digital authoritarianism or separating specific political and economic driving forces. However, other forces clearly affect the diffusion of digital authoritarianism (Morgus, 2019, p. 89). Specifically, the Chinese model provides working examples of digital surveillance and control systems. Since China argues for a more controlled digital sphere and "successfully" utilizes technology for authoritarian practices, regimes such as Türkiye are able to follow suit with relatively low investments and risks. Indeed, Türkiye ultimately wishes to establish national platforms and services similar to China and Russia (Topak, 2019, p. 11). On the other hand, the Russian model provides an alternative "low-cost" pathway for the same goals. Since authoritarian regimes "exchange tools and expertise for Internet control and promote ideas on how to govern digital technologies at the international

level." (Michaelsen & Glasius, 2018, p. 3788). In the end, Türkiye cherry-picks from these two models to create its own model following these technological and normative examples. Accordingly the Türkiye's authoritarian surveillance assemblage, where widespread surveillance is centralized at the hands of the government hierarchically (Topak, 2019, p. 4), shows similarities to both the Chinese and Russian models.

Conclusion

The use of digital technologies by authoritarian regimes to exercise control over the public, or digital authoritarianism, is on the rise due to both technological affordances and the general trend towards regulating the digital sphere. While it is not possible to pinpoint the active promotion of digital authoritarianism, it has a tendency to spread and deepen in the international system. The research on authoritarian diffusion generally struggles to differentiate between domestic pressures and international influence (Buzogány, 2017, p. 13). However, we argue that, unlike the diffusion of political practices and tendencies, the diffusion of digital authoritarianism is largely exempt from those research challenges. Since surveillance and the control of information primarily rely on technology, the patterns are easier to separate. Surveillance technologies provide more robust cases when combined with legal regulations and discourse, making the diffusion of digital authoritarianism become more clear.

The case of Türkiye demonstrates that the government borrows its normative foundations from China's internet sovereignty approach, focusing on limiting public dissent and strengthening the government's influence in the digital sphere. The Chinese model provides an encouraging template for authoritarian regimes, showing that the digital sphere does not have to be completely free for the creation of a thriving, innovative technology market as argued by Western democracies in the past. Instead, research suggests that in the case of advanced surveillance technologies such as artificial intelligence, authoritarian regimes have significant advantages over democracies (Karpa et al., 2022, p. 149). While this is an enticing example, China's unique advantages are not available to the rest of the world for direct emulation, and so achieving the same results with different strategies tailored to specific market forces, technological capabilities, and socioeconomic attributes gains importance.

The Russian model, with its popular national platforms and services with strong ties to the government, provides another example. Since Russia does not have the technological capacity or market to create an alternative national digital sphere similar to China's, focusing on control by other means is more feasible. This, in turn, makes the Russian model more practical for other states. However, Türkiye has no meaningful national digital platforms to

influence or bully into compliance like Russia. Since blocking access to global platforms would be devastating to the developing economy of Türkiye and would result in domestic and international political pressure, the regime initially struggled to create an effective functional strategy, resulting in ineffective or costly bans. More recent regulations show that the Turkish model is evolving towards less visible means of control, similar to Russia, while increasingly utilizing innovative tools and discourses for digital authoritarianism, like China.

The two models analyzed in this study both aim to create a digital sphere under the influence and control of the government. China achieved that goal by excluding global services, while Russia relied on the popularity of national services and took them under state control. When that was insufficient, Russia utilized populist mis/disinformation tactics to beat the opposition at its own game. Türkiye recently capitalized on global trends and created an alternative digital sphere within the global services by regulations. Since Turkish users cannot view critical content online, this has created an almost entirely separate sphere within the realm of the same services. This allows service providers to operate in the Turkish market, the government to access user information and manipulate the flow of information, and the public to access popular platforms with a wide variety of content while remaining unaware of censored critical content.

In conclusion, since there is no concrete evidence of the active promotion of authoritarian practices in the digital sphere, we argue that the diffusion of digital authoritarianism is an internally driven and passive process in the case of Türkiye. However, both the proof-of-concept and public opinion perspectives seem to be at play here. Türkiye utilizes technological affordances for surveillance and control in tandem with strict regulations built behind a façade of Western norms, similarly to both China and Russia, albeit with a tailored model fitting its own market forces and social structure. The Turkish model reflects the inspiration and acquisition of the technological prowess of China and the implementation of the low-tech alternatives and regulations of Russia. Combined with the compliance of global social media platforms due to their implementation of regulations due to fear of missing out, Türkiye's brand of digital authoritarianism keeps evolving alongside those of other authoritarian regimes towards stricter yet less visible means of control.

Further studies are required to analyze like-minded regimes, as the Turkish model is becoming another potential candidate to further expedite the diffusion of digital authoritarianism. Since most like-minded regimes do not enjoy the economic or technological affordances of either China or Russia yet aim to maintain and expand their control by utilizing

technology, the Turkish model may prove to be appealing. In this case, rigorous studies focusing on the various diffusion mechanisms are required to further shed light on this issue.

References

Akdeniz, Y. (2021, March 24). *Turkey: Twitter becomes latest company to comply with repressive social media law*. ARTICLE 19. https://www.article19.org/resources/turkey-twitter-becomes-latest-company-to-comply-with-repressive-social-media-law/

Akdeniz, Y. (2022, May 19). *Regulating disinformation and social media platforms "alla Turca."* ARTICLE 19. https://www.article19.org/resources/regulation-of-social-media-platforms-in-turkey-internet-law/

Akdeniz, Y., & Güven, O. (2020). *Fahrenheit 5651: Sansürün Yakıcı Etkisi*. Engelli Web. https://ifade.org.tr/yayinlar/rapor-kitap-calismalari/

Akyol, M. (2021, February 23). *Twitter might become inaccessible in Turkey as heftier penalty looms*. Expression Interrupted. https://www.expressioninterrupted.com/twitter-might-become-entirely-inaccessible-in-turkey-as-heavier-penalty-looms/

Allison, J. E. (2002). *Technology, development, and democracy: International conflict and cooperation in the information age* (J. E. Allison, Ed.). State University of New York Press.

Ambrosio, T. (2010). Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research. *International Studies Perspectives*, *11*(4), 375–392. https://doi.org/10.1111/j.1528-3585.2010.00411.x

Ambrosio, T. (2018). Authoritarian Norms in a Changing International System. *Politics and Governance*, *6*(2), 120–123. https://doi.org/10.17645/pag.v6i2.1474

Ambrosio, T., & Tolstrup, J. (2019). How do we tell authoritarian diffusion from illusion? Exploring methodological issues of qualitative research on authoritarian diffusion. *Quality & Quantity*, *53*(6), 2741–2763. https://doi.org/10.1007/s11135-019-00892-8

Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Barry, E. (2022, January 18). *These Are the Countries Where Twitter and Facebook Are Banned*. Time. https://time.com/6139988/countries-where-twitter-facebook-tiktok-banned/

Bradford, A. (2023). Exporting China's Digital Authoritarianism through Infrastructure. In A. Bradford, *Digital Empires* (1st ed., pp. 290-C8P73). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197649268.003.0009

Brewster, T. (2016, October 25). *Is An American Company's Technology Helping Turkey Spy On Its Citizens?* Forbes. https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan/

Brownlee, J. (2017). The limited reach of authoritarian powers. *Democratization*, *24*(7), 1326–1344. https://doi.org/10.1080/13510347.2017.1287175

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151

Bulman, M. (2016, November 4). *Whatsapp, Twitter and Facebook are now blocked in Turkey*. The Independent. https://www.independent.co.uk/news/world/asia/facebook-twitter-whatsapp-turkey-erdogan-blocked-opposition-leaders-arrested-a7396831.html

Burnay, M. (2019). Privacy and Surveillance in a Digital Era: Transnational Implications of China's Surveillance State. *EUCROSS*. https://ghum.kuleuven.be/ggs/research/eucross/eucross-wp-burnay-oct2019.pdf

Buzogány, A. (2017). Illiberal democracy in Hungary: Authoritarian diffusion or domestic causation? *Democratization*, *24*(7), 1307–1325. https://doi.org/10.1080/13510347.2017.1328676

Casier, T. (2022). Russia and the diffusion of political norms: The perfect rival? *Democratization*, *29*(3), 433–450. https://doi.org/10.1080/13510347.2021.1928078

Çetinkaya, O., & Güngördü, A. (2021, September 9). *When National Laws and International Standards Are at Odds: Human Rights Responsibilities of Social Media Platforms Under Turkey's New Internet Law* (United Kingdom). International Comparative Legal Guides; Global Legal Group. https://iclg.com/briefing/17140-when-national-laws-and-international-standards-are-at-odds-human-rights-responsibilities-of-social-media-platforms-under-turkey-s-new-internet-law

China: Freedom in the World 2023 Country Report. (2024). Freedom House. https://freedomhouse.org/country/china/freedom-world/2023

Clarke, S. (2021, March 24). *Turkey: Twitter becomes latest company to comply with repressive social media law*. ARTICLE 19. https://www.article19.org/resources/turkey-twitter-becomes-latest-company-to-comply-with-repressive-social-media-law/

Clayton, M. R., Kjerulf-Thorgeirsdottir, H., van DIJK, M. P., Benedek, M. W., & Turk, K. (2016). *On Law No. 5651 On Regulation of Publications on the Internet and Combating Crimes Commited by Means of Such Publication ("The Internet Law")*. EU COMMISSION for Democracy Through Law. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e

Coşkun, G. B. (2021). *Turkey's New Internet Law and Its Effects on Freedom of Media*. Reset Dialogues on Civilizations.

Deibert, R. J. (Ed.). (2008). *Access denied: The practice and policy of global Internet filtering*. MIT Press.

Derakhshan, H. (2015, December 29). Iran's blogfather: Facebook, Instagram and Twitter are killing the web. *The Guardian*. https://www.theguardian.com/technology/2015/dec/29/irans-blogfather-facebook-instagram-and-twitter-are-killing-the-web

Eldem, T. (2020). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration*, *43*(5), 452–465. https://doi.org/10.1080/01900692.2019.1680689

Ermoshina, K., & Musiani, F. (2021). The Telegram ban: How censorship "made in Russia" faces a global Internet. *First Monday*. https://doi.org/10.5210/fm.v26i5.11704

Eroğlu, D. (2022a, July 21). Belgeleriyle BTK-gate (1): Türkiye'deki tüm kullanıcıların internet hareketleri, yaklaşık bir buçuk yıldır, kimlikleri ve kişisel verileriyle birlikte BTK'ya akıyor. *Medyascope*. https://medyascope.tv/2022/07/21/belgeleriyle-btk-gate-turkiyedeki-tum-kullanicilarin-internet-hareketleri-yaklasik-bir-bucuk-yildir-kimlikleri-ve-kisisel-verileriyle-birlikte-btkya-akiyor/

Eroğlu, D. (2022b, July 26). Belgeleriyle BTK-gate (2): Toplanan kişisel veriler nasıl kullanılabilir? | Fişleme, siyasi manipülasyon ve daha fazlası. *Medyascope*. https://medyascope.tv/2022/07/26/btk-gatele-toplanan-kisisel-veriler-nasil-kullanilabilir-profilleme-fisleme-siyasal-manipulasyon-ve-daha-fazlasi/

Eroğlu, D. (2022c, August 2). Belgeleriyle BTK-gate (3): BTK-gate'in önceki gözetim girişimlerinden farkı ne? *Medyascope*. https://medyascope.tv/2022/08/02/belgeleriyle-btk-gate-3-btk-gatein-onceki-gozetim-girisimlerinden-farki-ne/

Esen, B., & Gumuscu, S. (2016). Rising competitive authoritarianism in Turkey. *Third World Quarterly, 37*(9), 1581–1606. https://doi.org/10.1080/01436597.2015.1135732

Feldstein, S. (2019). The Global Expansion of AI Surveillance. *Carnegie Endowment for International Peace*.

Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *International Affairs*, *97*(6), 1925–1944. https://doi.org/10.1093/ia/iiab146

Gilardi, F. (2016). Four Ways We Can Improve Policy Diffusion Research. *State Politics & Policy Quarterly*, *16*(1), 8–21. https://doi.org/10.1177/1532440015608761

Hall, S. G. F., & Ambrosio, T. (2017). Authoritarian learning: A conceptual overview. *East European Politics*, *33*(2), 143–161. https://doi.org/10.1080/21599165.2017.1307826

Holmes, R. (2013, September 3). *Have Social Networks Killed the Web?* https://www.linkedin.com/pulse/20130903164924-2967511-have-social-networks-killed-the-web/

Jamil, S. (2021). The rise of digital authoritarianism: Evolving threats to media and Internet freedoms in Pakistan. *Journal of Russian Media and Journalism Studies*, *3*(3), 5–33. https://doi.org/10.30547/worldofmedia.3.2021.1

Janofsky, A. (2020, February 14). *Can the US build its own 5G to compete with Huawei?* Protocol. https://www.protocol.com/huawei-5g-american-alternative

Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, *30*(2), 71–89. https://doi.org/10.1353/sais.2010.0006

Karpa, D., Klarl, T., & Rochlitz, M. (2022). Artificial Intelligence, Surveillance, and Big Data. In L. Hornuf (Ed.), *Diginomics Research Perspectives: The Role of Digitalization in Business and Society* (pp. 145–171). Springer. https://doi.org/10.1007/978-3-031-04063-4

Kedzie, C. (1997). *Communication and Democracy: Coincident Revolutions and the Emergent Dictators*. RAND.

Kenez, L. (2022, January 29). *TikTok reassures Turkish government that it will fully cooperate on legal requests—Nordic Monitor*.

https://nordicmonitor.com/2022/01/tiktok-reassures-turkish-government-that-it-will-fully-cooperate-on-legal-requests/

Kerr, J. A. (2018). Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region. *International Journal of Communication*, *12*(1), 3814–3834.

Kneuer, M., & Demmelhuber, T. (2016). Gravity centres of authoritarian rule: A conceptual approach. *Democratization*, *23*(5), 775–796. https://doi.org/10.1080/13510347.2015.1018898

Lee, Y. (2022). Can Digital Authoritarianism Deter Political Freedom?: Innovation in Digital Technology and Democratization. *The Korean Journal of International Studies*, *20*(1), 21–53. https://doi.org/10.14731/kjis.2022.04.20.1.21

Lokot, T. (2018). Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices. *Surveillance & Society*, *16*(3), 332–346. https://doi.org/10.24908/ss.v16i3.6967

Lührmann, A., & Lindberg, S. I. (2019). A third wave of autocratization is here: What is new about it? *Democratization*, *26*(7), 1095–1113. https://doi.org/10.1080/13510347.2019.1582029

Maggetti, M., & Gilardi, F. (2016). Problems (and solutions) in the measurement of policy diffusion mechanisms. *Journal of Public Policy*, *36*(1), 87–107. https://doi.org/10.1017/S0143814X1400035X

Marczak, B., Dalek, J., McKune, S., Senft, A., Scott-Railton, S., & Deibert, R. (2018, March 9). *BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?* The Citizen Lab. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Marrow, A. (2021a, May 17). Russia partially halts punitive Twitter slowdown, warns other tech platforms. *Reuters*. https://www.reuters.com/technology/russia-partially-lifts-restrictions-twitter-after-some-banned-content-deleted-2021-05-17/

Marrow, A. (2021b, December 3). CEO of Russia's VK resigns as state assumes control of internet firm. *Reuters*. https://www.reuters.com/article/russia-vk-idCNL8N2SO3IY

Matheson, E. (2020). *UAE Adoption of Digital Authoritarianism Weakens US Security and Portends Soft Power Shift*. Center for Anticipatory Intelligence Student Research Reports. https://www.usu.edu/cai/files/studentpaper-matheson.pdf

Meseguer, C., & Gilardi, F. (2009). What is new in the study of policy diffusion? *Review of International Political Economy*, *16*(3), 527–543. https://doi.org/10.1080/09692290802409236

Michaelsen, M., & Glasius, M. (2018). Authoritarian Practices in the Digital Age. *International Journal of Communication*, *12*(1), 3788–3794.

Morgus, R. (2019). *The Spread of Russia's Digital Authoritarianism* (Artificial Intelligence, China, Russia, and the Global Order). Air University Press.

Morgus, R. (2022). *The Spread of Russia's Digital Authoritarianism*. 10.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. MIT Press.

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130. https://doi.org/10.1111/1468-2346.12189

Peterson, D. (2020). *Designing Alternatives to China's Repressive Surveillance State*. Center for Security and Emerging Technology. https://doi.org/10.51593/20200016

Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models* (Democracy and Disorder). Brookings.

Qiang, X. (2021, August 4). Chinese Digital Authoritarianism and Its Global Impact. *POMEPS Studies*. https://pomeps.org/chinese-digital-authoritarianism-and-its-global-impact

Qin, A., Liu, J., & Chien, A. C. (2022, July 14). China's Surveillance State Hits Rare Resistance From Its Own Subjects. *The New York Times*. https://www.nytimes.com/2022/07/14/business/china-data-privacy.html

Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts, 5651, Turkey (2022).

Reuters. (2021a, May 26). Facebook, Twitter told to open databases in Russia by July -Ifax. *Reuters*. https://www.reuters.com/technology/russia-force-facebook-twitter-open-databases-russian-territory-by-july-ifax-2021-05-26/

Reuters. (2021b, June 28). Russia hits Big Tech with new charges for not deleting content - report. *Reuters*. https://www.reuters.com/technology/russia-hits-big-tech-with-new-charges-not-deleting-content-report-2021-06-28/

Reuters. (2021c, July 1). Putin signs law forcing foreign social media giants to open Russian offices. *Reuters*. https://www.reuters.com/technology/putin-signs-law-forcing-foreign-it-firms-open-offices-russia-2021-07-01/

Risse, T., & Babayan, N. (2015). Democracy promotion and the challenges of illiberal regional powers: Introduction to the special issue. *Democratization*, *22*(3), 381–399. https://doi.org/10.1080/13510347.2014.997716

Russia: Freedom in the World 2023 Country Report. (2024). Freedom House. https://freedomhouse.org/country/russia/freedom-world/2023

Sacks, S. (2018, January 29). New China Data Privacy Standard Looks More Far-Reaching than GDPR. *Center for Strategic & International Studies*.

https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr

Sarı, M. Ş. (2020, September 29). *What's Behind Turkey's New Internet Law?* Heinrich-Böll-Stiftung. https://tr.boell.org/en/node/21327

Shahbaz, A. (2018, October). *The Rise of Digital Authoritarianism*. Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

Sherman, J. (2021). Digital Authoritarianism and Implications for US National Security. *The Cyber Defense Review*, *6*(1), 107–118.

Sinkkonen, E., & Lassila, J. (2020). *Digital authoritarianism in China and Russia: Common goals and diverging standpoints in the era of great-power rivalry* (294). FIAA Briefing Paper.

Soldatov, A., & Borogan, I. (2013). Russia's Surveillance State. *World Policy Journal*, *30*(3), 23–30. https://doi.org/10.1177/0740277513506378

Tanash, R. S., Chen, Z., Thakur, T., Wallach, D. S., & Subramanian, D. (2015). Known Unknowns: An Analysis of Twitter Censorship in Turkey. *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, 11–20. https://doi.org/10.1145/2808138.2808147

Tansey, O. (2016). The problem with autocracy promotion. *Democratization*, *23*(1), 141–163. https://doi.org/10.1080/13510347.2015.1095736

The Internet in China. (2010). Information Office of the State Council of the People's Republic of China. http://www.china.org.cn/government/whitepaper/node_7093508.htm

Tolstrup, J. (2015). Black knights and elections in authoritarian regimes: Why and how Russia supports authoritarian incumbents in post-Soviet states: Black knights and elections in authoritarian regimes. *European Journal of Political Research*, *54*(4), 673–690. https://doi.org/10.1111/1475-6765.12079

Toor, A. (2014, April 22). *Russia's largest social network is under the control of Putin's allies, founder says*. The Verge. https://www.theverge.com/2014/4/22/5638980/russias-largest-social-network-is-under-the-control-of-putins-allies

Topak, Ö. E. (2019). The authoritarian surveillant assemblage: Authoritarian state surveillance in Turkey. *Security Dialogue*, *50*(5), 454–472. https://doi.org/10.1177/0967010619850336

Turkey: Freedom in the World 2022. (2022). Freedom House. https://freedomhouse.org/country/turkey/freedom-world/2022

Turkey: Freedom in the World 2023 Country Report. (2024). Freedom House. https://freedomhouse.org/country/turkey/freedom-world/2023

Twitter. (2022, July 28). *Sharing our latest transparency update, marking decade long commitment*. Twitter Blog. https://blog.twitter.com/en_us/topics/company/2022/ttr-20

Ünver, A. (2018). The Logic of Secrecy: Digital Surveillance in Turkey and Russia. *Turkish Policy Quarterly*, *17*(2).

Wang, E., & Shepardson, D. (2022, June 17). TikTok moves U.S. user data to Oracle servers. *Reuters*. https://www.reuters.com/technology/tiktok-moves-us-user-data-oracle-servers-2022-06-17/

Way, L. A. (2015). The limits of autocracy promotion: The case of Russia in the 'near abroad': The limits of autocracy promotion. *European Journal of Political Research*, *54*(4), 691–706. https://doi.org/10.1111/1475-6765.12092

Weyland, K. (2017). Autocratic diffusion and cooperation: The impact of interests vs. ideology. *Democratization*, *24*(7), 1235–1252. https://doi.org/10.1080/13510347.2017.1307823

Wong, J. C. (2016, July 15). Social media may have been blocked during Turkey coup attempt. *The Guardian*. https://www.theguardian.com/world/2016/jul/15/turkey-blocking-social-facebook-twitter-youtube

Yakouchyk, K. (2019). Beyond Autocracy Promotion: A Review. *Political Studies Review*, *17*(2), 147–160. https://doi.org/10.1177/1478929918774976

Yayboke, E., & Brannen, S. (2020). *Promote and Build a Strategic Approach to Digital Authoritarianism*. Center for Strategic and International Studies (CSIS).

Yesil, B., Sözeri, E. K., & Khazraee, E. (2017). *Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance*. The Internet Policy Observatory.

Yilmaz, G., & Eliküçük Yıldırım, N. (2020). Authoritarian diffusion or cooperation? Turkey's emerging engagement with China. *Democratization*, *27*(7), 1202–1220. https://doi.org/10.1080/13510347.2020.1777984

Zittrain, J., & Palfrey, J. (2008). Internet Filtering: The Politics and Mechanisms of Control. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Cinnamon (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 29–56). MIT Press.

Как Telegram-каналы стали инструментом власти. (2018, November 28). Проект. https://www.proekt.media/narrative/telegram-kanaly/