LSE Ideas

Against the Grain: The data regulatory regimes of Kazakhstan and Uzbekistan vis-à-vis Russia, China, and Big Tech

KENDDRICK CHAN, ENYI CHEN, MATTHEW HENEGHAN, DALYA SOFFER, POOMTHAWAT WACHIRAPORNPRUET

Digital IR | Working Paper Series

Executive Summary

Given the relative proximity of Central Asia to Russia and China, the Central Asian states of Kazakhstan and Uzbekistan have extensive military ties with Russia, in addition to playing a significant role in China's Belt and Road (BRI) and Digital Silk Road (DSR) initiatives. However, when it comes to cyberspace regulation and policy diffusion pathways, we find that the data policies of both Kazakhstan and Uzbekistan differ from their Russian or Chinese counterparts—particularly with regards to data sovereignty and data localisation are pertinent to Kazakhstani and Uzbekistani policymakers. This divergence is most notable with Kazakh and Uzbek approaches to US-headquartered Big Tech companies. The data regulatory regimes of Kazakhstan and Uzbekistan engage in a 'balancing act', involving a mix of strict data laws observed in Russia and China on one side, and various compliance agreements with Big Tech companies on the other. Additionally, we find that while Kazakhstan and Uzbekistan may seek to exercise their agency in data policy *formulation*, they nonetheless remain constrained by technical limitations regarding policy *implementation*. All of this contributes to a dynamic operational environment that is constantly in flux, which carries implications for Big Tech companies looking to conduct operations in Central Asia.

INTRODUCTION

Political regime transformation, rapid demographic growth, and the delivery of expansive infrastructure projects along the Digital Silk Road (DSR) have highlighted Central Asia as an emerging challenge for Big Tech companies. Half of the population across respective Central Asian states now has access to and uses the internet, and deepening internet penetration can be expected as the region's population grows by an estimated 23 million by 2050.[1] At the domestic level, increasing digitalisation has run parallel to the emergence of distinct cyberspace-oriented regulatory environments over the past decade. These regulatory environments are geared towards mitigating new political risks posed by the cyber domain—such as the role that various digital platforms (including those developed by Big Tech companies) might potentially play in exacerbating existing societal fault lines and fostering civil unrest. Kazakhstan and Uzbekistan are telling examples of the domestic regulatory environments developing across the region due to their attempts to balance increasing digitalisation with what policymakers perceive as privacy and national security risks.[2] However, the conventions of international observers to rationalise these tendencies by looking to intra-regional policy diffusion pathways—namely in relation to Russia's totalising crackdown on Big Tech companies—neglect the identification of divergent origins for digital policy environments of Central Asian states. While both Kazakhstan and Uzbekistan have enacted a series of policies intended to increase control of user data and the free flow of information across national borders, the turn toward *data sovereignty* and *data localisation* practices as explanatory phenomena threatens to oversimplify our expectations for how operational settings for Big Tech companies are likely to evolve.

Additionally, central to the development of these pathways is the ongoing disambiguation between data sovereignty and data localisation practices, each conceptually differentiated through hardening government discourse on the meta properties of citizen-generated information. Where data sovereignty broadly refers to recent government tendencies to proclaim legal jurisdiction over any data located within national borders, data localisation strictly mandates that the storage and usage of citizen-generated data must take place domestically with corresponding law enforcement.[3]

Table 1: Conceptualising the differences between 'data localisation' and 'data sovereignty'[4]

Data Sovereignty vs	Data Localisation
• Nominal declaration of state jurisdiction over citizen data or data created within physical borders • Weak or poorly defined legal regulations that are not actionable for data-handling organisations • Lack of surveillance mechanisms for ascertaining data generated within state jurisdiction and detecting violations • Lack of regulatory and legal organs for pursuing prosecution of data-handling organisations when alleging violations	• Substantive declaration of state jurisdiction over citizen data or data created within physical borders enshrined in law • Legally binding rules administered by regulatory bodies issued to data-handling organisations for compliance • Developed surveillance mechanisms and government bodies for monitoring cross-border data transfers and detecting possible violations • Dedicated legal entities to issue court proceedings against data-handling organisations found to have knowingly or unknowingly violated laws

[1] "Individuals Using the Internet (% of Population) - Europe & Central Asia", *Worldbank.org*, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=Z7, accessed 10 April 2022.

[2] For example: Jaclyn Kerr, "Authoritarian Practices in the Digital Age| Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region", *International Journal of Communication,* 12 (2018): 3814-3834.

[3] Dan Svantesson, "Data Localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301 (Paris: OECD Publishing, 2020).

[4] Compiled by authors.

Given the amount of data being generated and the associated privacy and security concerns, laws and regulations pertaining to data have become a pressing concern for policymakers worldwide.

Following the 2016 adoption of the European Union's (EU) General Data Protection Regulation (GDPR), the European Data Protection Board (EDPB) was set up in 2018 to foster inter-agency cooperation between the EU's numerous data protection authorities and ensure that data regulations are consistently applied throughout the Union.[5] Preceding this, Russia and China ratified their own data localisation laws, albeit driven by different imperatives. These include establishing substantial revenue flows to domestic hosts as foreign companies operating in Russia must rent data servers, while also mandating that private companies must decrypt any encrypted data about Russian citizens at the request of security services if users are suspected of engaging in "extremist" activities.[6] For states like Russia or China, which have poor track records for upholding civil liberties and human rights, there is a tendency for laws and regulations to become an 'instrument of the state'—in other words, a legitimised means for enforcing state authority over citizen behaviour—with data laws and regulations within those states being no different. While data regulatory regimes in Kazakhstan and Uzbekistan appear to lean to the 'stricter' side of the spectrum, there remains enough space for Big Tech companies to conduct their in-country business with relative ease.

To better understand these dynamics, this paper will explore the intricacies of how these regulatory environments have developed. In doing so, it will examine how domestic changes have transformed the modus operandi for Big Tech companies in the region and suggest how their relationship with such states is likely to evolve moving forward.

EVOLUTION OF REGULATORY POLICIES AND CYBERSPACE

Kazakhstan

Since the collapse of the Soviet Union, Kazakhstan has adopted a foreign policy approach that many characterise as a balancing act between competing global forces. Following its declaration of independence in 1991 and throughout the late 20th century, Kazakhstan sought to balance its security relationship with Russia with active involvement in the US-initiated NATO Partnership for Peace programme.[7] China and Russia are Kazakhstan's largest trading partners and both have taken steps to consolidate their presence in the country and in Central Asia more generally.[8] In addition to maintaining their economic dominance within Central Asia, both Russia and China have attempted to secure their influence in the region through various multilateral partnerships and security agreements, such as Russia's Eurasian Economic Union (EAEU) and China's Belt and Road Initiative (BRI).

Although both Russia and China have managed to demonstrate to Kazakhstan the economic value of Russo-Kazakh and Sino-Kazakh ties, Kazakhstan nonetheless exercises a delicate foreign policy that does not exclusively abide by the interests of these two geopolitical heavyweights. While Kazakhstan does not implement policies that would jeopardise financial and security assistance from Russia and China, it still retains a comparatively strong rapport with the West.[9] Through its active participation in the C5+1 multilateral dialogue forum (involving the foreign ministers of five Central Asian states and the US), Kazakhstan has

[5] Denis Kelleher and Karen Murray, *EU data protection law*, (London: Bloomsbury Professional, 2018).

[6] Markku Lonkila, Larisa Shpakovskaya and Philip Torchinsky, "The occupation of Runet? The tightening state regulation of the Russian-language section of the Internet" in *Freedom of Expression in Russia's New Mediasphere*, eds. M. Wijermars, & K. Lehtisaari, (Routledge, 2020), pp. 17-38.

[7] Martha Brill Olcott, Kazakhstan: *Unfulfilled Promise?* (Revised Edition), (Carnegie Endowment for International Peace, 2010).

[8] Iskander Akylbayev, "What Kazakhstan Can Teach About Medium-State Diplomacy." *Foreign Policy*, https://foreignpolicy.com/2021/05/04/what-kazakhstan-can-teach-about-medium-state-diplomacy/ (2021), accessed 21 September 2022.

[9] Wilder Alejandro Sanchez, *A Rising Global Player: Kazakhstan's Foreign Policy in the 2020s*, (Wilson Center, 2020).

signalled its openness to the US having stronger ties with the region. The country has also worked with the US to enhance cooperation on strategic issues. Given the ongoing US-China rivalry as well as tensions between Russia and the West, the above developments are signs of Kazakhstan adopting a hedging strategy where it maintains its strategic relationships with both China and Russia while avoiding weakening ties with the US.[10]

The 'balancing act' adopted by Kazakhstan in its relationship with China, Russia and the West is mirrored in the country's cyber governance regimes. Kazakhstan has taken significant steps toward investing in digital programmes and infrastructures to expand state control. The government has proactively increased its digital surveillance capacity over the last few years.[11] Being a significant partner in China's BRI and DSR initiatives, Kazakhstan sought to cooperate extensively with information and communications technology (ICT) companies from China to expand its digital control over Kazakh citizens. For instance, Chinese ICT companies have helped with the implementation of Safe City projects, which employ facial recognition cameras, data management systems, and control centres to gather information and track the activity of the Kazakh population.[12]

The Kazakh government has also implemented strict data localisation laws to manage data in the country, which closely resemble related policies in Russia and China. Since 2005, the country has required any website using the Kazakh domain ".kz" to host its information locally. Since this law was passed, the government has refused applications to register any ".kz" domain for a firm that does not comply with the domestic data localisation laws.[13] In 2016, Kazakhstan expanded its data localisation requirements by mandating that all personal data sourced within Kazakhstan be stored locally, a regulation which bore resemblance to Russia's data localisation laws. Kazakhstan's largest internet service provider, Kazakhtelecom, is also state-owned, which grants the Kazakh government effective control of the country's internet infrastructure.[14] Other telecommunication companies that seek to establish operations in the region therefore need to connect their service through Kazakhtelecom's infrastructure. This offers the Kazakh government a firm grip over content monitoring as well as censorship capabilities. Through these various pathways, the government can easily block access to websites (and prevent the Kazakh population from viewing the information contained within) and services that are out of line with its guidelines and principles. All of this demonstrates how Kazakhstan's digital framework and regulatory environment are reflective of strict government control—a development that is arguably facilitated and influenced by both China and Russia.

However, it is also important to highlight that, contrary to popular belief, the digital governance protocols of Kazakhstan do not reflect those of Russia and China in their entirety. Unlike Russian or Chinese authorities who have initiated sweeping crackdowns on US-headquartered Big Tech companies or have banned them from operating within the country, Kazakh authorities have attempted to strike a balance by seeking to forge agreements with tech companies to get them to comply with local regulations, rather than forcing them out of the region altogether.[15] Many Big Tech companies (e.g., Google, Meta) have managed to strike such deals with Central Asian governments, which allows their associated digital platforms (e.g., Instagram, Facebook) to operate in-country, albeit under the condition that they comply with local regulations. For instance, Facebook recently authorised Kazakh government access to Facebook's "Content Reporting System", enabling the government to flag and report content that they deem to be in violation of local laws.[16] In another instance,

[10] *Ibid.*

[11] Cian Stryker, 'Digital Silk Road and Surveillance Technology in Central Asia', in D*igital Silk Road in Central Asia: Present and Future*, eds. by Nargis Kassenova and Brendan Duprey, (Cambridge: Davies Center for Russian and Eurasian Studies, 2021), pp. 17–54.

[12] *Ibid.*

[13] Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, (Information Technology & Innovation Foundation, 2017).

[14] "Freedom on the Net 2020: Kazakhstan", *Freedom House* www.freedomhouse.org/country/Kazakhstan/freedom-net/2020 (2020), accessed 21 September 2022.

[15] Akylbayev, (2021).

[16] Catherine Putz, "Facebook Grants Kazakhstan Direct Access to Content Reporting System", *The Diplomat* https://thediplomat.com/2021/11/facebook-grants-kazakhstan-direct-access-to-content-reporting-system/ (2021), accessed 10 September 2022.

the Kazakh government recently passed a bill mandating that such companies are required to have in-country offices in order to operate within the country.[17] Although these examples serve to demonstrate the extent of the grip that the Kazakh authorities have over information and content-reporting, such policies are best described as *conditionally restrictive*, rather than *wholly prohibitive*. In a manner analogous to the country's foreign policy, Kazakhstan again performs the 'balancing act'. It imports technology infrastructure and derives inspiration for technology governance from China and Russia, yet provides US-headquartered Big Tech companies room to operate within the country.

Uzbekistan

Uzbekistan has been amongst the countries with the most extensive cyberspace regulatory regimes. Uzbek authorities have adopted policies that promote state control over data and its cross-border flow, including the incremental move towards data localisation. Uzbek digital data regulation dates back to the mid-2000s, when the government mandated that all internet connections to the outside world must go through a single international gateway provided by Uztelecom, a state-owned company.[18] In 2011, Uzbekistan also joined Russia, China, and Tajikistan at the United Nations to propose the International Code of Conduct for Information Security,[19] emphasising the sovereign right of each state's digital information environment, for both the data itself and the associated communication systems. This development signifies the explicit desire of Uzbek authorities to 'wield the mantle of data sovereignty'. Finally, in 2019, the Uzbek parliament passed a new law prescribing that all personal data be stored domestically, and that all ICT companies within the country must operate on locally registered servers.[20]

Although conventional belief holds that this digital policy follows a model pioneered by Russia and China,[21] [22] [23] laying out developments in the digital regulations in a chronological manner suggests that such claims might not solely explain the evolution of digital policies within Uzbekistan. While Uzbekistan has a history of aligning itself with Russia and China on the international stage,[24] this steady progress of control over the flow of data and digital information, tacit proclamations of data sovereignty, and data localisation practices suggest that Uzbekistan is exercising its own agency in this regard. This sharply contrasts with conventional wisdom that Uzbekistan is a mere recipient of the digital governance model that great powers in its near-abroad have been trying to export to. However, it should also be noted that while Uzbekistan arguably has independently formulated digital regulatory policies, Uzbek authorities might nonetheless find themselves limited by their capacity to implement such policies. Due to Uzbekistan's relative lack of technical expertise and equipment, the government remains constrained between what it *aspires to do* (as evidenced by its formulated policies) and what it *might actually be able to do*. For instance, the Uzbek government relies largely on Soviet-era measures

[17] "Meta Denies Kazakh Claim of Exclusive Access to Facebook's Content Reporting System", Reuters https://www.reuters.com/world/asia-pacific/facebook-lets-kazakh-govt-directly-flag-harmful-content-joint-statement-says-2021-11-01/ (2021), accessed 10 September 2022.

[18] "Freedom on the Net 2016: Uzbekistan", Freedom House https://freedomhouse.org/sites/default/files/FOTN%202016%20Uzbekistan.pdf (2016), accessed 19 July 2022.

[19] Jing de Jong-Chen, "Data Sovereignty, Cybersecurity, and Challenges for Globalization", Georgetown Journal of International Affairs, 16 (2015): 112-122.

[20] Ulugbek Abdullaev and Eldor Mannopov, "Uzbekistan: Data localization requirement to be effective in April 2021", JD Supra www.jdsupra.com/legalnews/uzbekistan-data-localization-3000241 (2021), accessed 19 July 2022.

[21] Nargis Kassenova and Brendan Duprey, "Introduction" in Digital Silk Road in Central Asia: Present and Future, eds. by Nargis Kassenova and Brendan Duprey, (Cambridge: Davies Center for Russian and Eurasian Studies, 2021), pp. v–vi.

[22] Miranda Lupion, "Sino-Russian Advocacy for 'Internet Sovereignty' and State-Led Internet Governance" in *Digital Silk Road in Central Asia: Present and Future*, eds. by Nargis Kassenova and Brendan Duprey, (Cambridge: Davies Center for Russian and Eurasian Studies, 2021), pp. 9–16.

[23] Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders: How a Group of Often Overlooked Countries Could Hold the Keys to the Future of the Global Internet", New America https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/ (2018), accessed 19 July 2022.

[24] Lupion, (2021).

for telecommunication systems monitoring,[25] and a significant portion of its digital infrastructure is provided by Chinese state-owned enterprises through various DSR projects.[26] Considering Uzbekistan's limited capacity and capability regarding policy implementation, it remains unlikely that the country will be able to formulate policies that fail to take its big power neighbours, Russia and China, into the calculus.

IMPLICATIONS FOR BIG TECH: COMPLY OR BE PUNISHED

As discussed in previous sections, data regulation laws have been in place in both Kazakhstan and Uzbekistan since the 2000s. However, in the time since, such laws have become increasingly stringent in parallel with the increased ability of state authorities to sanction tech companies for non-compliance. Data localisation laws are increasingly an instrument of statecraft that authorities use against tech companies—with little recourse for these companies in the event that they feel unfairly treated. However, there are limitations regarding the extent to which governments can utilise data localisation laws against Big Tech companies. Let us now explore the different ways in which data localisation has affected Big Tech companies and how the dynamics between the state and those companies have played out.

Data localisation creates additional costs for foreign tech firms operating within these states. Establishing and operating a localised data service requires staffing, training, engineering (i.e., development, maintenance, debugging), backup, and local physical infrastructure that meets certain standards to physically store data.[27] Priority must be given to data security systems to protect data and maintain data integrity in domestic environments where digital security and data protection remains relatively low. The relative lack of cybersecurity safeguards in Central Asian countries is a particularly acute problem, especially for tech companies operating there. For instance, cybersecurity and data protection are core concerns for both the Kazakh population and the Kazakh government, given that in 2019, a database containing information pertaining to approximately 11 million people was leaked from the Central Election Commission, resulting in a massive scandal.[28] Although it is argued that 'data sharding', or breaking up data into smaller chunks and distributing across data nodes, is a potential solution to ensuring data security, data localisation laws often prevent such 'sharding' of data. There have also been arguments that data localisation makes data more vulnerable to security attacks, rather than more secure.[29] Overall, data localisation laws are creating new risks and challenges for foreign tech firms.

Data localisation laws and their enforcement by the state has changed the nature and power dynamics of the relationship between the state and Big Tech companies. Through a slew of regulatory regimes (i.e., data localisation laws), the former has found its power increased even to the point of overreach, while the latter has found its autonomy relatively eroded. For companies, the choice is often between adaptation and compliance, or non-compliance and punishment. It is against this backdrop that we now highlight the different experiences Kazakhstan and Uzbekistan have had with their respective regulatory frameworks.

[25] Miranda Lupion, "The Sino-Russian Digital Cooperation and Its Implications for Central Asia" in *Digital Silk Road in Central Asia: Present and Future*, eds. by Nargis Kassenova and Brendan Duprey, (Cambridge: Davies Center for Russian and Eurasian Studies, 2021), pp. 55–76.

[26] Stryker, (2021)

[27] Roy Camp and Noémie Weinbaum, "Data Localisation - The Magic Bullet?", *McAfee* https://www.mcafee.com/blogs/blogs/enterprise/data-security/data-localisation-the-magic-bullet (2021), accessed 17 July 2022.

[28] "Freedom on the Net 2020: Kazakhstan", (2020).

[29] Frank Heidt, "The Harms of Forced Data Localization", Leviathan Security Group https://www.leviathansecurity.com/media/the-harms-of-forced-data-localization (2015), accessed 17 July 2022. A more comprehensive discussion on the opportunities, costs, and risks can be found in Svantesson's data localisation OECD paper: Dan Svantesson, (2020).

Kazakhstan

In Kazakhstan, mandating that tech companies comply with data laws and regulations has afforded the government the ability to exercise authority and control over the digital sphere. This development is most evident in the example of Facebook, which has given Kazakh authorities access to the company's "Content Reporting System", allowing the government to arbitrarily single out online content deemed to be in violation of the law and report it for subsequent removal from the social media platform. Facebook also held training sessions for Kazakh officials on other aspects of its platforms, such as the "Content Notification System", as well as the Facebook Content Policy and Community Standards. Such access was the result of a compromise following threats by Kazakh authorities to block the platform from operating within the country.[30] Following criticism from international audiences that the company was inadvertently empowering the Kazakh government's overreach by providing access to its content moderation systems, Facebook has argued that this process is not unique to Kazakhstan, and is actually consistent with its long-standing practice of allowing governments around the world to report content that is deemed to violate local law.[31] However, despite this justification, it is arguable that operating in Kazakhstan has led to certain legitimacy and reputational setbacks for Facebook—all of which serves as a lesson for foreign tech companies who wish to operate within the country. Using Facebook as a case study, it can be argued that content regulation legislation is a front for the additional centralisation of government power and authority as it enables easier removal of content that governments deem unfit. To date, there is evidence that Big Tech firms have opted to compromise and comply with the demands of the Kazakh authorities, despite the costs incurred to their autonomy and institutional reputation.

Uzbekistan

While the use of gateway control and internet shutdowns had regularly been adopted for censorship of political contents and other forms of digital activism in Uzbekistan under President Islam Karimov, the beginning of President Shavkat Mirzoyoyev's administration was characterised by political reforms and liberalisation.[32] The country had begun to foster a more friendly and conducive policy environment for Western tech companies after he assumed office. Beginning in 2018, reports suggested that some social networking platforms such as Skype and WhatsApp were gradually being allowed to operate on its network.[33] However, the new localisation legislation has created setbacks for this endeavour. In 2021, data localisation laws again forced service termination of several social networking platforms, including Skype, Twitter, TikTok, VKontakte, and WeChat.[34] Specifically, the government has cited the failure to comply with new localisation regulation as the reason for these punitive measures.[35]

The implication is that compared to past measures, this legislation now opens a more flexible, selective, long-term censorship that does not require shutting down the country's internet or slowing down connection, which Uzbekistan government has previously done.[36] Moreover, as it forces servers to be hosted within the country, localisation should also maintain the potency of the single gateway approach to data control in the face of planned relaxation of connectivity restriction, such as the introduction of private satellite internet.[37] In the end,

[30] "Meta and Kazakhstan spar over Facebook Control", Euractiv https://www.euractiv.com/section/central-asia/news/meta-and-kazakhstan-spar-over-facebook-control/ (2022), accessed 17 July 2022.

[31] "Meta Denies Kazakh claim of exclusive access to Facebook's content reporting system", *Reuters* https://www.reuters.com/world/asia-pacific/facebook-lets-kazakh-govt-directly-flag-harmful-content-joint-statement-says-2021-11-01/ (2021), accessed 17 July 2022.

[32] Maria A. Blackwood, *Reforms in Uzbekistan*, (Congressional Research Service, 2020).

[33] Stryker, (2021).

[34] "Uzbekistan Restricts Access To Several Social Media Sites", *Radio Free Europe/Radio Liberty* https://www.rferl.org/a/uzbekistan-restricts-social-media/31339492.html (2021), accessed 20 July 2022.

[35] *Ibid.*

[36] "Freedom on the Net 2016: Uzbekistan", (2016).

[37] "Freedom on the Net 2021: Uzbekistan", *Freedom House* https://freedomhouse.org/country/uzbekistan/freedom-net/2021 (2021), accessed 19 July 2022.

this could suggest that Uzbekistan's primary concern remains maintaining control over the internet rather than keeping its relationship with tech companies, especially when the two objectives are in conflict with each other. The government has chosen to simply ban them from the country outright when non-compliance happens instead of tolerating the presence of disobedient companies. Even if Big Tech companies wish to avoid complying with what they deem as excessive government demand and preserve their reputation, the ability of the government to revoke their licence to operate within the country leaves little room for them to bargain otherwise.

Nonetheless, it should also be noted that the government is by no means omnipotent or able to operate independent of outside factors, particularly when it comes to domestic popularity of the regime. While social media companies on their own are relatively unable to effectively resist the demands of the Uzbek government, there remains a pathway through which government overreach might potentially be curbed.

In late 2021, when the Uzbek government cracked down on some of the country's most popular platforms—including Telegram, Facebook, and YouTube—it faced a massive public outcry which eventually forced the Uzbek President to intervene and shift the blame to poor management of the state internet regulatory authority, Uzkomnazorat.[38] This was followed by the partial restoration of access to those services.[39] Twitter and TikTok, however, remain blocked.[40] This incident has shown that given a high enough level of internet penetration and social media usage, any shutdown might trigger an outcry from the now-disconnected populace and lead to a potential backlash against the government. This therefore limits the government's capacity to arbitrarily 'flip the switch' on the internet—albeit not completely eliminating the possibility.

CONCLUSION: THE WAY FORWARD

Whilst the focus of this paper has been on Kazakhstan and Uzbekistan, the trend for increased data protection regulations has proliferated across geographical boundaries. In 2021 alone, China, Russia, Saudi Arabia, Turkey, Kuwait, and the UAE all passed laws or amendments to national data protection regulations. Senegal, China, and Russia have passed data localisation laws, requiring the local storage of data.[41] Overall, the state-centric digital governance model continues to gain momentum—not just as a principle under debate but as a policy being practised. It has proven to be a viable approach: tech companies can either adapt and comply or be punished and told to cease all in-country operations. This sets a solid precedent for countries aiming to push forward localisation laws. Furthermore, this also means that states remain preeminent actors in dictating governance policy and practice, capable of exerting influence over Big Tech when the agenda requires.

However, it might be too presumptuous to say that this will become the global norm at this stage, especially considering that governments seek legitimacy from the populace and are cognisant that enacting what the populace deems arbitrary and excessive control could be detrimental to the regime. Given that transnational data flows have been core to the operations of Big Tech companies, it is certain that the dynamics will be in constant flux as battles, debates, and compromises over digital data flows ensue. ■

[38] "Head of Uzkomnazorat Fired for Illegally Blocking Social Networks in Uzbekistan", *Kun.uz* https://kun.uz/en/news/2021/11/03/head-of-uzkomnazorat-fired-for-illegally-blocking-social-networks-in-uzbekistan (2021), accessed 20 July 2022.

[39] Joanna Lillis, "Uzbekistan: Outraged Netizens Win Partial Victory over Social Media Blocks", *Eurasianet* https://eurasianet.org/uzbekistan-outraged-netizens-win-partial-victory-over-social-media-blocks (2021), accessed 19 July 2022.

[40] *Ibid*.

[41] "The 2021 Data Regulation Recap", *InCountry* https://incountry.com/blog/the-2021-data-regulation-recap/ (2021), accessed 18 July 2021.

The Authors

Kenddrick Chan is the Deputy Head of the Digital International Relations project at LSE IDEAS.

Enyi Chen is an MSc International Relations student at the London School of Economics and Political Science and Research Assistant at LSE IDEAS.

Matthew Heneghan is an MSc International Social and Public Policy student at the London School of Economics and Political Science and Research Assistant at LSE IDEAS.

Dalya Soffer is an MSc International Relations student at the London School of Economics and Political Science and Research Assistant at LSE IDEAS.

Poomthawat Wachirapornpruet is an MSc International Relations student at the London School of Economics and Political Science and Research Assistant at LSE IDEAS.