Freedom House

Kazakhstan

FREEDOM ON THE NET 2020

NOT FREE

32
/100

A. Obstacles to Access	10 /25
B. Limits on Content	11 /35
C. Violations of User Rights	11 /40

LAST YEAR'S SCORE & STATUS
32 /100 Not Free

Scores are based on a scale of 0 (least free) to 100 (most free)

Overview

Internet freedom in Kazakhstan remains under threat. In July 2019, the government rolled out its national security certificate, a machine-in-the-

middle (MITM) technology enabling it to monitor users' online activities. Facing outcry, President Kassym-Zhomart Tokayev halted the certificate's rollout after a few weeks, but its basis in legislation remained untouched, which means that it can be reintroduced at any time. The government also moved during the coverage period to implement advanced video surveillance technologies, even as multiple high-profile data breaches raised concerns over the security of citizens' personal data. In the fall of 2019, numerous users were temporarily disconnected from the internet when the government disabled unregistered mobile devices, while throughout the coverage period, emergency situations and unauthorized political gatherings were accompanied by localized internet shutdowns. Online content continued to be censored, while users—in particular, journalists who work online—continued to face legal and extralegal attacks.

President Tokayev, a former diplomat and senator, was elected in June 2019 in a vote that, according to international observers, was marred by fraud. Nursultan Nazarbayev, Kazakhstan's long-serving first president, retained the title Leader of the Nation and control over the powerful Security Council—along with legal immunity and other privileges—after his resignation in March 2019. Nazarbayev's position has created a dual power structure in the country, which in turn has created uncertainty over who exactly is in charge. Tokayev promised to institute reforms early in his presidency, but no serious changes have occurred to date. Outside of elite circles, political competition is nonexistent, as the authorities strictly control the public sphere, showing little tolerance for opposition political parties or independent media.

Key Developments, June 1, 2019 - May 31, 2020

- President Tokayev's June 2019 election was marked by sizable protests. The state responded by restricting connectivity in major cities and violently arresting demonstrators as well as journalists (see A3 and C7).

- In July 2019, the government debuted the Qaznet Trust Certificate, a machine-in-the-middle (MITM) technology enabling it to monitor users' online activities, before reversing course amid domestic and international outcry (see C5).
- In the fall of 2019, the government began to disable unregistered mobile devices, temporarily disconnecting those users who had not linked their devices' International Mobile Equipment Identify (IMEI) codes with their state-issued IDs (see A3 and C4).
- In December 2019, President Tokayev pledged to decriminalize defamation, a charge that has historically been used to suppress critical voices. He did not fulfill this pledge until June 2020, after the coverage period (see C2).

A. Obstacles to Access

The government has solidified its grip on the information and communication technology (ICT) sector through substantial investments, including direct subsidies to the state-run monopoly Kazakhtelecom. During the coverage period, the government disrupted internet connections during political protests staged by the opposition, riots, and other emergency situations. The rollout of the IMEI code registration system further disrupted connectivity, if only temporarily.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**5** / 6

Internet access has increased significantly over the past decade. According to the most recent official data, 84.2 percent of the population used the internet in 2019, a 2.9 percent increase over 2018. [1] In February 2019, the state statistical agency reported a 5.5 percent decline in the number of fixed-line internet subscriptions relative to 2018, [2] but by May 2020 this figure had rebounded 3.7 percent. [3] This trend, along with the continued increase in overall internet penetration, is a sign that more people are connecting to the internet via mobile devices. Of the 24.5

million active mobile subscriptions in Kazakhstan as of May 2020—accounting for a 131.5 percent mobile penetration rate—14.7 million are used to access the internet. [4]

The government's Digital Kazakhstan program has already met its goal of increasing the internet penetration rate to 82.3 percent by 2022. [5] The country's mobile networks continue to expand, but 3G services are available to only 88 percent of the population, and 4G services to just 75 percent, according to the Economist Intelligence Unit's 2020 Inclusive Internet Index. [6] Several mobile service providers piloted fifth-generation (5G) services during the coverage period.

According to May 2020 testing data from Ookla, the average download speed of a fixed-line connection in Kazakhstan was 44.1 Mbps, while the average download speed of a mobile connection was 20.9 Mbps (both slight increases over previous measurements). [7] Connection speeds in Kazakhstan compare favorably to those of other Central Asian countries. However, speeds dipped during the COVID-19 pandemic, as more users went online more often. [8]

Most people access the internet from their mobile devices at home and at work, and in various public places in cities where high-speed internet is often available free of charge via Wi-Fi hotspots at cafés and libraries.

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2** / 3

Both mobile and fixed-line internet connections remain relatively affordable. According the International Telecommunication Union (ITU), in 2019, a monthly fixed broadband subscription cost around 1 percent of gross national income (GNI) per capita, while a monthly mobile data subscription offering 5GB of data cost 0.4 percent of GNI per capita. [1] The Economist Intelligence Unit's 2020 ranking of 100 economies in terms of the affordability of prices for internet connections placed Kazakhstan 28th, ahead of other Central Asian countries. [2] However, a

national currency devaluation following the collapse of global oil prices, [3] along with an overall economic downturn associated with the COVID-19 pandemic, [4] negatively affected affordability, even though service providers had not raised prices by the end of the coverage period. The government also distributed cash payments to compensate citizens for lost income. However, citizens had to apply for these payments online, creating difficulties for those without digital skills or reliable access to the internet. [5]

Many operators provide free, unbilled access to popular social media platforms and messaging apps as part of prepaid plans. In addition, amid the COVID-19 pandemic, all major mobile service providers offered free, unbilled access to online educational resources, [6] and in some cases they allowed their subscribers to access internet resources even if subscribers could not pay their account balances. [7]

Internet access is more limited in rural areas, where about 42 percent of the population resides. [8] As part of the Digital Kazakhstan program, the government pledged in late 2018 to invest 60 billion tenge ($160 million) in fixed-line internet connections for villages, benefiting 2.4 million rural residents over three years. This work, performed via public-private partnership schemes, is under way to connect one-third of all villages via fiber-optic technology and the rest via WiMax (Worldwide Interoperability for Microwave Access) base stations. [9] Prices for the connections in villages are expected to match those in cities, [10] despite the fact that the average monthly salary is substantially lower in the countryside.

Internet access is distributed relatively evenly across Kazakhstan's ethnic communities. All public institutions are required to provide at least Kazakh and Russian versions of their websites, and many private-sector entities follow this example. The country has started transitioning from the Cyrillic alphabet to the Latin alphabet, with the stated aim of modernizing the Kazakh language by reducing the number of letters and making it compatible with most encoding and fonts for digital communications. [11]

Gender does not seem to be a barrier to internet access in Kazakhstan. [12]

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**1** / 6

During the coverage period, connections were repeatedly limited or disabled altogether in an apparent attempt to prevent political protests or the dissemination of information during emergency situations. The practice of throttling social media platforms has become common, but episodes are typically brief or localized, allowing them to remain important forums for online discussion.

During antigovernment protests triggered by the death of activist Dulat Agadil in police custody in February 2020 (see C7), mobile networks were disrupted in Almaty and the capital Nur-Sultan on March 1, 2020. [1]

In February 2020, a local internet shutdown was recorded in the Korday district amid an outbreak of intercommunal violence between ethnic Kazakhs and the Dungan minority. In addition, at the same time, the government temporarily blocked WhatsApp in a bid to stop the violence. [2]

Access to a variety of social media platforms and messaging apps, including several Google services like Gmail and YouTube, was also temporarily restricted. [3] Some speculated that the restrictions were an attempt to suppress discussion of the late Aisultan Rakhat, a grandson of former president Nazarbayev, who had announced that he was seeking asylum in the United Kingdom [4] and that his family had been embezzling funds from the country's oil revenues. [5]

The outlawed opposition party Democratic Choice of Kazakhstan (DVK) staged rallies in February 2020 to protest obstacles to its registration; mobile networks were reportedly disrupted in the areas around these demonstrations. [6]

In October 2019, an unknown number of users were disconnected from the internet after the authorities enabled a database of IMEI codes;

service was cut off to mobile devices that were not registered in the database. In 2017, the government had required users to register their devices' IMEI codes before the end of 2018 (see C4). This requirement, presented by authorities as motivated by the need to crack down on counterfeit and stolen devices, [7] effectively enabled security services to connect users' personal identification numbers (which are also linked to users' SIM cards) and IMEI codes. The database is operated by the State Radio Frequency Service. According to a spokesperson for state-owned mobile operator Kcell, the disconnection of devices in October 2019 was a test. [8] Users were able access the internet again after registering their devices.

In September 2019, local disruptions of mobile networks were also observed in connection with DVK rallies in Almaty and Nur-Sultan. [9]

Extensive disruptions took place during and after Kazakhstan's snap presidential election on June 9, 2019, affecting news sites, [10] social media platforms, and messaging apps. [11] On June 12, 2019, the day of President Tokayev's inauguration, a major shutdown affected social media platforms, messaging apps, and, reportedly, banking systems, which disabled electronic payments for a short period of time. [12] Mobile operators acknowledged that their services had been suspended but denied responsibility. [13]

That same month, local internet disruptions occurred following a massive explosion at an ammunition depot in Arys. Minister of Digital Development, Innovation, and Aerospace Industry Askar Zhumagaliev blamed the disruptions on infrastructure failures caused by the blast. [14] However, many users speculated that the disruptions were deliberately imposed to slow the spread of firsthand information during the emergency situation.

On a number of occasions during the coverage period, most notably in June 2019 [15] and February 2020, [16] President Tokayev personally intervened to end internet disruptions.

A number of legal mechanisms allow the government to suspend telecommunications networks at will. According to a 2018 decree, the

Ministry of Defense, the Ministry of Internal Affairs, the Prosecutor General's Office, and the National Security Committee (NSC) have priority access to telecommunications networks as well as the right to suspend those networks in an emergency, or the risk thereof. Experts have voiced concerns about the decree's vague terminology—particularly "social emergency situation" and "risk of emergency situation." [17] The decree does not specify limits on the duration of network suspensions.

The NSC has controlled the State Technical Service (STS) since 2017, [18] assuming the authority to block content and disrupt internet networks for investigative purposes and to "prevent crimes." The NSC can act without a court order, though it must notify other state bodies within 24 hours. [19] In 2017, the NSC and a number of other state entities adopted new rules for blocking or suspending networks, ICT resources, and other web resources. The rules are classified. [20]

A 2016 law empowers the NSC to suspend "networks and means of communication and access to the internet" in "urgent cases that may result in commitment of grave or especially grave crimes." The NSC is not required to obtain prior approval to do so and can subsequently inform the Prosecutor General's Office and the relevant regulator—the Ministry of Digital Development, Innovation, and Aerospace Industry, as of 2020. [21]

Since 2014, the Prosecutor General's Office has also been authorized to issue orders to shut down communications services without a court order if "networks are used for felonious aims to damage interests of individuals, society or state," including the dissemination of illegal information and calls for extremism, terrorism, mass riots, or participation in unauthorized public gatherings. [22] Orders must be executed by either telecommunications companies or the STS within three hours.

In 2012, amendments to the Law on National Security allowed the government to forcibly suspend telecommunications during antiterrorist or riot-suppression operations. [23]

The government centralizes internet infrastructure in a way that facilitates control of content and surveillance. State-owned Kazakhtelecom, through its operations and a number of subsidiaries, holds a de facto monopoly on

the country's backbone internet infrastructure. The NSC's supervision of the STS allows it to exercise control over peering centers and international gateways. [24] Amendments enacted in 2017 made the management of cross-border internet exchange points (IXPs) a state monopoly in the name of "information security." [25] In February 2019, KazNIC, the nonprofit registry for the country's .kz domain, announced the launch of an independent IXP, but it offers peering only of domestic, not international, traffic. [26]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**2** / 6

While the government does not actively keep new players out of the ICT market, it did little to prevent the merger of Kazakhtelecom with two major mobile service providers in 2019, securing a 60 percent share in the mobile market. [1] Now, Kazakhtelecom's only major competitor is the foreign-owned firm Beeline Kazakhstan, which commanded 40 percent of the mobile market at the end of 2019. [2]

There are several significant internet service providers (ISPs) in Kazakhstan, but Kazakhtelecom holds a dominant market position. As of April 2019, it controlled 69 percent of the fixed-line market and 62 percent of the mobile market share. [3] It also fully or partially owns a number of other backbone and downstream ISPs. The state owns 45.9 percent of Kazakhtelecom through Samruk-Kazyna, its sovereign wealth fund. [4] Furthermore, Skyline Investment Company, a Luxembourg-incorporated firm whose beneficial owners are linked to the Nazarbayev family, [5] owns 22 percent of Kazakhtelecom. [6]

All mobile operators were given the right in 2016 to offer 4G services. [7] Since mid-2018, the government and mobile service providers have been moving toward the introduction of 5G services; pilot tests have taken place in Almaty and Nur-Sultan. [8] Kazakhtelecom indicated its intention to become the sole 5G provider in Kazakhstan, [9] but Beeline—lobbying

for an even field for all operators—was reportedly in talks as of 2019 regarding a 5G license and held a three-month 5G trial in Shymkent. [10]

Companies providing telecommunications services require an operating license from the Ministry of Digital Development, Innovation, and Aerospace Industry's Telecommunications Committee under the Law on Permissions and Notifications. [11] The Law on National Security limits foreign ownership of companies providing telecommunications services. [12] Moreover, these companies are required to purchase and install equipment related to the state's System for Operational Investigative Measures (SORM), a lawful interception apparatus (see C5), and to bear costs related to data-retention obligations (see C6). These companies are also required to cover costs related to the database of IMEI codes (see A3) [13] and to pay regular fees to the State Radio Frequency Service, which is the IMEI database operator. These obligations may deter new players from entering the ICT market.

No special licensing is required for businesses that decide to set up Wi-Fi hotspots.

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

The Ministry of Digital Development, Innovation, and Aerospace Industry is responsible for the telecommunications sector (including ICT infrastructure), e-government, and cybersecurity. The Ministry of Information and Social Development oversees mass media, including online content. Until the first half of 2019, both online content and the telecommunications sector were supervised by the now-defunct Ministry of Information and Communication. [1] Ministers are nominated by the prime minister and appointed by the president. The ministries' operations are not transparent or subject to independent oversight.

The NSC has increased its power to make decisions about ICT infrastructure and online content. In 2018, a cybersecurity entity called the

National Coordination Center for Information Security was launched under the NSC's supervision; [2] its workings remained secret. The leadership of the NSC is appointed by the president in coordination with the chair of the Security Council, a position occupied by former president Nazarbayev for life. [3]

The Internet Association of Kazakhstan (IAK), established in 2009, claimed to be an umbrella institution for the industry and a self-regulatory body, [4] although some have questioned the group's independence, transparency, and nonprofit status. [5] The IAK is currently idle. No other internet-related organization represents a serious counterweight to the government.

The .kz country domain is managed by the nonprofit KazNIC registry. The Kazakhstan Association of IT Companies administers domain names and regulates KazNIC tariffs. A 2015 law granted the government the power to appoint both the registrar and the domain name administrator. Though the government made no changes to the incumbent personnel, some experts expressed concern that this power may be abused. [6]

B. Limits on Content

Although the coverage period saw the state impose fewer new restrictions on content, continued censorship and media manipulation, often under the pretext of combating "extremism," marred the online public sphere.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	**2** / 6

The government has extensive authority to block online content. Online resources such as messaging apps that many in Kazakhstan use to share news—notably, Telegram—were periodically blocked during the coverage period.

There are no publicly available data on the extent of state censorship, although one unofficial estimate puts the number of blocked websites at more than 30,000 (see B3). The Ministry of Information and Social Development, responding to an access to information request, specified that 61 webpages were blocked by court order in 2019, including 17 for illegal gambling, 22 for terrorism and extremism, and 14 for sharing patently false information. Meanwhile, 21,267 webpages were blocked administratively, including 17,000 for terrorism and extremism. Propaganda of violence or suicide, pornography, and drug dealing were also among top five reasons given for blocking webpages. [1]

Users who wish to circumvent censorship tend to use virtual private networks (VPNs), but many anonymizing tools have themselves been blocked, and other tools frequently experience service problems. [2] The authorities have confirmed that they can block VPNs using court decisions or orders from the Ministry of Information and Social Development (see B3). [3] ProtonMail and Tor were blocked during the coverage period. [4]

The authorities have several times—fewer than in previous coverage periods—blocked or interfered with social media platforms and messaging apps like Telegram. ISPs and authorities have typically attributed disruptions to ill-explained technical issues. These restrictions have typically taken place during antigovernment demonstrations and emergency situations (see A3). For example, on the day of Kazakhstan's snap presidential election (June 9, 2019) and for days after, users in several cities where antigovernment demonstrations took place found that social media platforms and messaging apps—including Facebook, Instagram, and WhatsApp—were temporarily inaccessible. [5]

In May 2020, the DVK-affiliated human rights website Kuresker) was blocked, just weeks after it was launched. Kazakhtelecom and several state bodies denied responsibility for the blocking. [6]

Petition websites Avaaz.org, Change.org, and GoPetition.com remained inaccessible during the coverage period. They were blocked in previous years for hosting open letters that condemned government policies. [7] International media outlets like the *Daily Mail*, Kyrgyzstan's Kloop, and the

Russian-language Meduza remained inaccessible during the coverage period.

SoundCloud, a platform for podcasts and music, was blocked in 2018 for hosting extremist and terrorist materials. [8] Local advocacy organization Internet Freedom Kazakhstan urged authorities to unblock it. The Ministry of Information and Social Development ran tests on the platform and restored access to it in October 2019 upon finding no traces of illegal content. [9] This case demonstrates one imperfection of the current practice of website blocking: entire platforms are often blocked for isolated posts or accounts, with the platforms remaining inaccessible even when these posts or accounts have been removed.

Coub, a video platform, was blocked in 2018 for hosting extremist materials; it remained inaccessible throughout the coverage period. [10] Other hosting websites were intermittently or permanently unavailable during the coverage period, including Archive.org and Issuu.

Access to many social media platforms and an array of other internet resources was interrupted by introduction of the national security certificate for several weeks during the summer of 2019 (see C5). Some, but not all, users attempting to connect to social media platforms like Facebook, OK, Twitter, and VKontakte (VK), as well as websites such as Mail.ru and YouTube, were denied access unless they installed the certificate.

Ratel.kz, an independent news website that had been banned from operating in 2018, was allowed to resume operations in November 2019, after the expiration of the court-ordered ban (which entailed the blocking of its domain). [11]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	**1** / 4

The authorities use various nontechnical means to enforce the removal of content, including direct pressure on outlets to take down specific material and similar requests aimed at international social media platforms. There is no up-to-date information on the quantity of removals, only sporadic reports. In November 2019, the Ministry of Information and Social Development revealed that more than 25,000 “illegal materials” were deleted by website owners or administrators in 2019. [1] The government has not disclosed more recent statistics.

Tilda, a Russia-based platform for designing and hosting websites, was blocked in July 2019 in a bid to remove pornographic content from a single site. [2] Some 42,000 websites—including those of independent news outlets, businesses, and nonprofits—were blocked at once, as they shared the IP addresses of Tilda’s cloud hosting service. Tilda released a statement saying the company cooperates with government requests to remove illegal content but had not received any requests from Kazakhstani authorities. [3] When access to Tilda was restored after about a week, the allegedly pornographic website was no longer accessible. This case prompted criticism of the practice of blocking by IP address and the government’s lack of communication with online platforms.

Facebook and Twitter’s transparency reports have no record of removal requests from the Kazakhstani government in the latter half of 2019. [4] However, during that period, Google received 24 takedown requests from the government—mostly because the materials were deemed defamatory or for national security reasons—targeting 28,498 items. Google removed only 0.6 percent of the 28,498 items; 3.8 percent had already been removed, while a further 0.6 percent could not be found. [5] In all, the company kept 95 percent of the items up.

In 2016, the Ministry of Information and Communication adopted new rules for the monitoring of media, including social media, using the planned Automated System of Monitoring the National Information Space [6] to uncover illegal content online. The authorities have continued to conduct manual monitoring since then [7] ; the automated system—in development since 2017—had been expected to be in use by the end of

2019. [8] It is unclear if the system, which reportedly cost $4.5 million, has been introduced. [9]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**1** / 4

While the legal framework and procedures for blocking websites and removing content did not change during the coverage period, the government has greatly expanded its authority to censor the internet in recent years, and extralegal blocking remains a common practice. All website blocking and content removal procedures lack transparency.

Former Minister of Information and Social Development Dauren Abayev had, while in office, repeatedly declared that his ministry did not block websites and that, in the event that certain websites are inaccessible, users should blame ISPs. [1] For their part, ISPs do not accept blame for website blocking; the STS, overseen by the NSC, has the ability to block websites on its own.

According to Kazakhstan's Mass Media Law, [2] all internet resources, including websites and pages on social media platforms, are considered media outlets. Under 2014 amendments to the law, the Prosecutor General's Office is authorized to order ISPs to block content without a court order. ISPs must comply with such requests until the website owner deletes the content in question. The law provides no leeway for an ISP to reject the order or for the website owner to appeal. [3] In 2016, the Ministry of Information and Communication gained the authority to issue takedown and blocking orders until website owners remove specific content. The NSC has the right to suspend access to websites or information they host "in cases of emergency that may result in criminal actions" autonomously and need only notify the Prosecutor General's office and regulator afterward.

By equating all internet resources with media outlets, the Mass Media Law makes web publishers—including bloggers and social media

users—liable for the content they post, but the law does not specify whether publishers are responsible for content posted by third parties. In 2015, the Ministry of Information and Communication stated that social media users could be held liable for extremist comments posted on their pages by third parties, as permitting the publication of extremist materials in a mass media outlet is an offense under the criminal code that can be punished with up to 90 days in jail.

Amendments to the Communications Law in 2016 obliged ISPs to monitor content passing through their networks and to decide whether to restrict any problematic material. [4] The amendments do not specify how ISPs are to carry out this obligation. The administrative code in force since 2016 imposes fines on ISPs for not complying with censorship orders. [5]

In order to avoid having a website or page permanently blocked and to escape legal liability, owners of internet resources must remove content that is deemed extremist or is otherwise banned. Once illegal content is identified, ISPs and the STS must suspend access to the entire website within three hours. The party responsible for the content then receives a request for its removal; if the party complies, ISPs and the STS must unblock the website. [6]

Websites can also be blocked by court order, even in the absence of the defendant's representative. No notification—to the public or the website owner—about the reason for the blocking is required. The courts frequently issue orders to block websites, banning dozens at a time, mostly on the grounds of religious extremism. The appeals procedure is opaque and has yet to be tested. An individual must apply for judicial approval simply to view court rulings on blocking cases. [7]

In 2017, the Ministry of Information and Communication launched a pilot version of a blocked websites roster, which users could check to determine whether a website was blocked by a court decision or government order, or to complain about disturbing online content. [8] Many blocked websites were not listed. According to Internet Freedom Kazakhstan, more than 30,500 international and Kazakhstani domains were blacklisted as of May 2020. [9]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Self-censorship in the media is pervasive, even among independent online news outlets. [1] The climate of self-censorship also extends to private businesses. However, after the resignation of President Nazarbayev in 2019, many users have visibly become more outspoken in online discussions—mainly on Facebook—even as most generally avoid a range of taboo topics. Online media workers continue to test boundaries, despite facing legal harassment and real-world violence (see C3 and C7).

A 2017 law prohibits anonymous online comments (see C4). [2] Although this ban is loosely observed, it limits the space for free speech on popular news sites that comply with the requirement.

The designation of the DVK as an illegal extremist organization prohibits any mention of the banned party that does not note its status as an extremist organization.

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**1** / 4

Compared with print and broadcast media, the online media landscape in Kazakhstan is subject to less overt forms of restrictions on the free flow of information, such as progovernment propaganda and pressure to self-censor (see B4). While social media platforms remain the most liberal setting for the public exchange of news and opinions, online discourse is prone to manipulation, including by commentators paid by the government. [1] According to one analysis, the activities of paid commentators (dubbed Nurbots, after former president Nazarbayev) serve to distract internet users in times of crisis and to play up the state's

successes. Three of Kazakhstan's most popular domestic online news outlets (as of March 2019) are owned by the government, while six more have a progovernment bent, according to research from the Center for Media, Data, and Society at Central European University. [2]

During the COVID-19 pandemic, President Tokayev called on the Ministry of Information and Social Development, the Prosecutor General's Office, and other state bodies to "pay close attention to the dissemination of rumors and provocative reports." [3] The pandemic did generate a wave of misinformation, [4] as local social media influencers spread conspiracy theories about COVID-19. [5]

Authorities have cultivated close ties to social media influencers. Some observers alleged in 2019 that Salem Social Media, a video production company in Kazakhstan helmed by a former spokesperson for the ruling Nur Otan party, [6] may receive government funding [7] and buy off bloggers. [8] Similar practices are reportedly employed at the provincial level. [9] During the coverage period, Salem Social Media's sister company, BTS Digital, reportedly consulted with the government to develop an app similar to China's WeChat. Vice Minister of Digital Development, Innovation, and Aerospace Industry Abylaikhan Ospanov confirmed the government's interest in a domestic social media platform [10] but denied any public funding for such a project. [11]

In April 2019, Factcheck.kz issued a report on the government-sponsored troll farm Smmnetwork LLC. The investigation revealed the existence of a network of fake accounts that could be connected to the First President's Foundation, a powerful state-funded institution established by former president Nazarbayev in 2000. [12] According to researchers at Oxford University, the government and political parties use both automated and human-run social media accounts to amplify friendly narratives, discredit the political opposition, and distract ordinary users from sensitive issues. [13] During the coverage period, progovernment accounts on various social media platforms waged a smear campaign against the Kazakhstan International Bureau for Human Rights and Rule of Law, a domestic human rights organization, after it publicly opposed a new law restricting freedom of assembly. [14] In addition, the municipal government of Nur-

Sultan signed a contract with the firm Dasco DataCom to promote its image online, including by responding to negative online materials. [15]

Officials, civil servants, and employees of state-owned companies are obliged to follow a set of guidelines on their use of the internet. These guidelines urge them not to post or repost materials that are critical of the government and not to "friend" the authors of such materials in order to preserve the image of the public sector and prevent the dissemination of false information or leaks. [16]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**1** / 3

Most major nonstate online news media outlets are affiliated with government officials or business figures with ties to the government. These outlets are likely to be recipients of government procurement contracts to produce favorable reporting. Indeed, many outlets, including domestic privately owned blogging platforms, are frequent recipients of such contracts. [1]

In 2019, the government planned to spend nearly 36 billion tenge ($97 million) on media contracts; several billion more was to be distributed less transparently by provincial and local administrative bodies. [2] For example, more than 380 million tenge ($1 million) was spent by the East Kazakhstan regional administration on media contracts, with nearly a third of those funds going toward social media advertisements. [3] The Legal Media Center, a nongovernmental organization focused on media rights, sued the Ministry of Information and Communication to demand information about the contracts, but a court rejected the case in January 2018, citing "commercial secrecy." [4] Overall, the volume of state media contracts has exceeded the overall advertising market for several years in a row. [5]

Online news media are not required to register with the government. There are no serious restrictions on their access to advertising, but

periodic blocking discourages businesses from placing ads on independent news sites. Furthermore, the digital media market in Kazakhstan, as in many other countries, is quite small. According to the IREX 2019 Media Sustainability Index, most media in Kazakhstan depend on financing from their founders and owners or grants from international organizations. [6] Online outlets' ability to remain in business is also limited by certain regulations, including a 20 percent cap on foreign-owned stakes in any company. [7]

B7 0-4 pts

Does the online information landscape lack diversity?	**2** / 4

Despite the challenging business environment for independent outlets, a small number of respected and critical websites continue to operate in Kazakhstan. The restrictions on the online media market remain less severe than those on the traditional media sector.

In the 2020 Inclusive Internet Index, Kazakhstan placed 52nd out of 100 countries surveyed in terms of the "existence and extent of local language content and relevant content" on the internet. [1]

International social media and communications platforms are accessible and popular, although connectivity is sometimes restricted (see B1). YouTube, VK, and Wikipedia are among the top sites in Kazakhstan. [2] According to Accenture Kazakhstan, a consulting company, more than 70 percent of Kazakhstani adults use social media platforms, with Facebook and YouTube commanding the largest audiences. [3]

Users can freely access most international news platforms, but only a small percentage of Kazakhstanis consume content in English. While there is much more domestic online content available in Russian than in Kazakh, including on news portals and social media, the volume of Kazakh-language content is gradually increasing.

Tools like VPNs are widely used to circumvent sporadic blocking, and there appears to be some semiofficial acknowledgment of this fact. When

asked about Kazakhstan's website blocking regime at the 2019 Eurasian Media Forum, Aleksandr Aksyutits, the head of Salem Social Media (see B5), dismissed the impact of the blocking by noting that people can use VPNs to access restricted sites. [4]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**2** / 6

The use of social media platforms and other digital tools for civic and political organizing is quite limited in Kazakhstan. Popular platforms are subject to periodic restrictions, particularly ahead of and during demonstrations. Discussions of political or social issues on social media platforms are often eclipsed by sensationalist content that is widely shared online.

The authorities sometimes block messaging apps ahead of protests to prevent users from accessing group chats to coordinate protest actions, including those run by the banned opposition DVK party. Informants have infiltrated critical groups on Telegram and other platforms to build cases for prosecutions. At the end of April 2019, the Prosecutor General's Office warned that organizing "unauthorized" demonstrations on "social networks and instant messengers" constitutes a violation of Article 488 of the code of administrative offenses. [1] The office issued similar warnings throughout the coverage period. [2] (All public demonstrations in Kazakhstan must receive permission from the authorities.)

Online petition websites are blocked to prevent campaigning (see B1). As a result, activists have turned to alternate platforms. An online campaign against redevelopment in historic downtown Almaty featured a petition hosted on Google Docs. It gathered 3,000 signatures, leading the city administration to cancel planned construction. [3]

In early 2019, the Ministry of Public Development announced its intention to create an official petition platform, [4] but the process was put on hold because of reorganization of the cabinet. In February 2020, the Ministry of

Information and Social Development announced it was developing a service called E-petition that would enable citizens to create petitions and sign them with certified electronic signatures. [5]

Police routinely summon activists ahead of planned protests to warn them against holding demonstrations, intimating that they will face consequences. [6] For example, several activists from a grassroots proreform movement called Oyan, Kazakhstan were taken by police from their homes during the morning of March 1, 2020, the day the group had planned to stage a rally in Almaty. They were released five hours later. [7]

C. Violations of User Rights

During the coverage period, there were fewer prosecutions of users than in previous years, but government pressure on online media ramped up significantly. The government moved to enhance its surveillance powers at the expense of users' privacy, including through introduction of the national security certificate.

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**1** / 6

The constitution guarantees freedom of expression, but this right is qualified by other laws and severely restricted in practice by prohibitions on defamation, publication of false information, and other speech-related offenses (see C2).

Although internet resources are deemed mass media outlets, bloggers do not enjoy the same rights as journalists, and even formally employed journalists face numerous restrictions on their work. In February 2019, for example, the Ministry of Information and Communication said it would further restrict journalists' already limited access to events at state bodies. [1] Police and progovernment thugs who harass bloggers and journalists

are seldom punished and enjoy de facto immunity. Nevertheless, the government's plan for the development of Kazakhstan's information sphere, adopted in April 2020, envisions raising the profile of bloggers, including by according them the right to be accredited by various government institutions as well as accorded the same protections traditional journalists enjoy in some circumstances. [2] The state has long been collaborating with select bloggers to generate positive coverage on social media platforms (see B5).

The president appoints all judges, and the judiciary is not independent in practice. The Constitutional Court was abolished in 1995 and replaced with the Constitutional Council, to which citizens and public associations are not eligible to submit complaints.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	**0** / 4

The government uses a number of provisions in the criminal code and the code of administrative offenses to restrict forms of online expression that may be protected under international human rights standards. [1] Vaguely worded legislation leaves ample space for interpreting criticism and opinions as defamation or extremism.

Article 174 of the criminal code prescribes up to 20 years in prison for the provocation of class, ethnic, national, religious, or social hatred. [2] Prosecutions under this provision are widespread, and human rights advocates have repeatedly voiced concerns about the lack of clarity in its terminology, especially the concept of "social" hatred. [3] Article 179 prescribes 5 to 10 years in jail for "propaganda or public calls" for the seizure of power or "forcible change of the constitutional order," when made using mass media or telecommunications, while Article 256 prescribes 7 to 12 years in jail for "public appeals to commit an act of terrorism" made through the same means. [4] Article 274 prohibits the dissemination of rumors or "knowingly false information that creates the danger of disrupting public order or causing substantial harm" to citizens,

organizations, or the state, which is also punishable by up to seven years in prison in the most extreme cases. [5]

Defamation and insult (Articles 130 and 131 of the criminal code, respectively) were criminal offenses during the coverage period, although shortly after the coverage period, the government moved to decriminalize defamation. [6] When it was a criminal offense, defamation could result in fines and up to three years in prison. [7] Insults may result in fines or up to 180 hours of correctional labor. [8] The criminal code provides stricter punishments for insulting state officials, judges, and members of the parliament. Desecration of the president's image and insulting the president or the president's family members are also criminal offenses (Article 373), punishable with a fine and up to three years in prison. [9] Government officials and progovernment business magnates have a history of using defamation and insult charges to punish critical reporting.

President Tokayev announced in December 2019 that he would move to decriminalize defamation and hate speech. [10] In March 2020, the government presented draft amendments to decriminalize defamation for public discussion. In June 2020, after the coverage period, the amendments were enacted, [11] moving defamation from Article 130 of the criminal code to the code of administrative offenses, so that it would entail a fine of $1,000 to $3,500 or 15 to 20 days of arrest. If the act of defamation was made publicly, via mass media, or in ICT networks, the fine increases to $1,200 to $4,200, and time in custody increases to 20 to 25 days. Under these amendments, Article 174 remains in the criminal code, although the word "provocation" was changed to "incitement," and fines ranging from $13,000 to $45,000 were introduced as an alternative to suspended sentences or prison terms of 2 to 20 years. [12]

In 2015, the Ministry of Information and Communication stated that social media users could be held liable for extremist comments posted on their pages by third parties, as this may be regarded as permitting the publication of extremist materials in a mass media outlet, an offense under Article 183 of the criminal code that is punishable by up to 50 days in jail. [13] Users who post or share such content may be fined for its "production, storage, import, transportation and dissemination," and in

some cases, jailed for up to 20 years under Article 174 of the criminal code. [14]

C3 0-6 pts

Are individuals penalized for online activities?	**2** / 6

Individuals are frequently penalized for online activities. According to the Legal Media Center, about 100 people are sentenced each year for posts made on social media platforms. [1]

In past years, the authorities routinely arrested and prosecuted individuals for posting critical commentary online, especially DVK-related online activities. The classification of the DVK as an extremist group made it illegal to disseminate its content online, including through private messages. [2] During the coverage period, a court ruled that the DVK-affiliated political movement Koshe Partiyasy ("Street Party") was also an extremist organization, arguing that it was, in fact, one and the same as the DVK. [3] However, compared with previous years, there were far fewer prosecutions for DVK-related online activities during the coverage period. Developments regarding the DVK during the coverage period included the following:

- In early 2019, DVK party member Aigul Akberdi was acquitted on charges of "calling for the violent overthrow of the government" via her participation in a DVK Telegram channel. [4] Her acquittal was overturned in April 2019, [5] but she remained free and continued her political activism. Her husband, Ablovas Jumayev, was sentenced to three years in prison in 2018 for sharing content in a DVK Telegram channel. [6] In July 2019, he was released after a court replaced the rest of his prison term with a suspended sentence. [7]
- In October 2019, two social media users were convicted of supporting the DVK on social media platforms, each receiving a one-year suspended sentence. One was also banned from using social media platforms for two years. [8] Several other cases in this vein were reported during the coverage period. [9]

- In March 2020, Azamat Baikenov, a political blogger from Petropavlovsk, was accused of participation in the DVK (an offense under Article 405 of the criminal code) for liking and commenting on DVK-related posts on social media platforms. He denies any connection to the banned movement and maintains that authorities use accusations of involvement with the DVK as a means to punish critics. [10]

During the coverage period, defamation and insult charges were extensively used to punish activists, bloggers, journalists, and ordinary users for critical online comments. According to the Prosecutor General's Office, in 2019, half of the 84 criminal prosecutions for defamation involved online defamation. [11] However, the media rights watchdog group Adil Soz identified only 26 prosecutions for defamation and insult in 2019 that violated free expression rights. [12] In the first five months of 2020, the group identified six more prosecutions. [13] The group's statistics do not differentiate between online and offline defamation and insult. Notable prosecutions include the following:

- Ordinary users Zhambyl Kobeisinov and Dilbar Begzhanova were sued by a police officer in the Mangystau region for defamation and insult, committed via YouTube video. In December 2019, they were cleared of insult charges but found guilty of defamation under Article 130 of the criminal code. Begzhanova received six months of probation, while Kobeisinov was sentenced to six months in jail. A court of appeals upheld the verdict in February 2020. [14]
- Arman Khassenov, a resident of the Karaganda region, was arrested for two months after he criticized former president Nazarbayev in a YouTube video. Charged by the NSC with insulting the president's honor and dignity, he faced up to three years in jail, [15] but in June 2020, he was given a three-year suspended sentence. [16]

At the same time, a number of cases during the coverage period pointed toward a growing rate of acquittals on defamation and insult charges. [17] In one case, Amangeldy Batyrbekov, a well-known journalist from southern Kazakhstan, was sentenced to 27 months in jail in October 2019 for a Facebook post that allegedly contained defamation of a senior local

official. [18] In January 2020, an appellate court acquitted him and ordered his immediate release. [19] He was then targeted by two other suits [20] and briefly detained in February 2020. [21]

Batyrbekov's ongoing saga highlights the renewed pressure placed on online media and individual journalists, which is especially noteworthy because internet-based media are the most significant sources of independent information in Kazakhstan. In July 2019, a reporter for Current Time TV, a subsidiary of Radio Free Europe/Radio Liberty (RFE/RL), was deported from Kazakhstan and banned from visiting the country for five years. [22] In February 2020, the government refused to accredit two RFE/RL journalists. [23]

During the coverage period, the authorities routinely used terrorism and extremism charges, including "provocation of hatred" (Article 174 of the criminal code), to prosecute online activity, [24] usually applying "restriction of freedom," or suspended sentences. [25] Local human rights advocates have criticized the lack of expertise among judges and prosecutors evaluating extremism or terrorism charges. [26] In 2019, Adil Soz recorded 99 pending cases under this article, but no prominent cases in court or court decisions. [27]

At the time of writing, at least 80 criminal cases had been opened for the dissemination of patently false information amid the COVID-19 pandemic, based on government monitoring of social media platforms and messaging apps. [28] (However, many of these cases will likely not reach court.) Ordinary users identified as authors of fake stories have been fined [29] or detained for three to five days. [30] A number of bloggers and journalists have found themselves facing such accusations for their reporting, although in at least one case the authorities ultimately declined to press charges. [31]

During the pandemic, several prominent activists were detained for disseminating patently false information during the state of emergency that was declared (Article 274 of the criminal code)—a crime that implies up to seven years in jail—and other offenses. In April 2020, Alnur Ilyashev, an outspoken critic of the government from Almaty, was arrested

for disseminating patently false information during the state of emergency even though his alleged offense preceded the state of emergency and had no relation to it. [32] Investigators determined one of his videos contained a “negative evaluation” of the ruling Nur Otan party that had damaged its reputation. [33] That same month, in Oral, blogger Aslan Sagutdinov was detained for “breach of quarantine.” He insists that he did not violate quarantine requirements as he was going from home to the grocery store, which is a permitted activity. He was detained for three days and later faced charges of disobeying and insulting a representative of authority. [34] Meanwhile, also in April, Almaty-based blogger Gennady Krestyanski was detained and charged with provocation of violation of order during the emergency situation. Reportedly, he was trying to film a guarded checkpoint on the city border and disobeyed the police. Krestyanski, who denies the charges, was detained for 10 days. [35]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**1** / 4

The government places restrictions on anonymous communication. Since December 2017, users have been required to identify themselves using government-issued digital signature technology or SMS (Short Message Service) verification in order to comment on domestic websites; [1] failure to enforce the rule can lead to fines. [2] Some news outlets and other sites introduced identification functionality in response to the requirement, but more simply disabled their comment sections, inviting readers to comment on social media platforms instead.

The government is cracking down on VPNs and other anonymizing tools with court orders. [3] For example, in March 2018, a court blocked the IPVanish VPN service. [4] Encryption tools are not restricted, but most users do not employ them.

SIM card registration is required for mobile phone users. The government also requires users to register all devices that use mobile networks—including mobile phones, tablet computers, and

smartwatches—with their mobile service providers, linking a person's government-issued identification, SIM card information, and device IMEI codes. Under 2018 legal amendments, unregistered mobile devices were to be disabled by service providers beginning in January 2019. [5] In February 2019, law enforcement bodies admitted that there had been multiple "technical problems" that would require mobile service providers to further modernize their networks. [6] In October 2019, the authorities enabled the IMEI code system, forcing operators to disable numerous unregistered devices (see A3). By law, operators are prohibited from providing services to clients with unregistered devices. [7]

Authorities presented the 2018 amendments as a means of fighting mobile device theft, counterfeiting, and terrorism. [8] However, human rights advocates warned of their effects on user privacy and their potential to enable surveillance by effectively linking personal ID numbers, SIM cards, and IMEI codes. [9] The technical capacity to disable a device was reportedly used to target activists during the protests during and after the 2019 presidential elections. [10]

Since 2016, users have had to obtain an SMS code to access public Wi-Fi networks. Such authentication potentially opens the door to surveillance because of the country's SIM card registration requirement. [11] Businesses can be fined up to 226,000 tenge ($600) for failing to comply with the new rules, while users can be fined up to 22,600 tenge ($60). [12] As of 2020, very few hotspots had introduced this system, and open access to public Wi-Fi networks remained the norm.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**2** / 6

It is difficult to estimate the scope of government surveillance in Kazakhstan, but digital rights groups allege that large-scale surveillance infrastructure is in place. The government employs SORM technology, which originated in Russia and is similar to that employed by other former Soviet countries, for deep packet inspection (DPI) of data transmissions,

among other functions. An investigation by the news site Vlast.kz published in February 2019 revealed a vast network of ties between Kazakhstan and Russia in the area of cybersecurity. [1]

In January 2018, new technical regulations for SORM developed by the NSC entered into force. [2] Sweden's Telia Company, which owned the mobile service provider Kcell (now a part of Kazakhtelecom), warned in 2017 that the impending new surveillance requirements gave the government real-time access to providers' networks, threatening freedom of expression. [3] Local human rights monitors have since alleged that law enforcement bodies and special services watch and wiretap phone conversations of opposition activists without following proper procedures. [4]

Various authorities monitor internet traffic. The STS is responsible for overseeing cross-border network traffic through a system called Centralized Management of Telecommunication Networks. All telecommunications service providers must be connected to this system and are required to grant authorities physical access to their control centers. [5] Kazakhtelecom, which maintains a DPI system separate from SORM, insists that it is used for traffic management and provides no access to users' personal data. [6]

In mid-July 2019, ISPs urged subscribers in Nur-Sultan to install a root security certificate called the Qaznet Trust Certificate, created by the state-run Qaznet Trust Network. The legal groundwork for introduction of the so-called national security certificate had been introduced in 2016, but no signs of the certificate's technical implementation were registered until July 2019. [7] ISPs warned that users might have difficulty accessing certain websites if they chose to skip installation of the certificate, even though it was not mandatory. [8] (What's more, according to researchers at the University of Michigan, the certificate only ever affected "a fraction of connections passing through the country's largest ISP, Kazakhtelecom." [9]) The certificate's introduction was justified as a means of fighting the theft of users' personal data, fraud, and other online threats, including cyberattacks. [10] The government stated that this "pilot

test" of the certificate was part of its Cybershield cybersecurity program. [11]

Commentators and experts inside the country and abroad almost unanimously considered the certificate a government-initiated technology for the interception of encrypted user traffic via MITM attacks. [12] Some of the 37 websites that University of Michigan researchers identified as targets of the certificate included Facebook, Gmail, Instagram, Mail.ru, OK, Twitter, VK, and YouTube, suggesting that its purpose was to "surveil users on social networking and communication sites." [13] The NSC admitted the certificate enables it to decrypt secure traffic but said it did not plan to store and view the details of citizens' online activities. [14]

Amid domestic and international outcry, Apple, Cisco, Google, and Mozilla stated that they would ban the Qaznet Trust Certificate from their respective web browsers (Safari, Chrome, and Firefox) to ensure that their users' personal data were not intercepted. [15] In early August 2019, the NSC declared that the certificate's trial period was over, claiming that the pilot test allowed it to test its cybersecurity systems as well as reveal and prevent millions of cybersecurity incidents. [16] It also informed users that they could remove the certificate. [17]

The authorities appear to engage in social media surveillance, including under the auspices of the Ministry of Information and Social Development [18] and via contractors such as Alem Research or IMAS, a private company that advertises a "monitoring system" that can "identify dangerous sources of social destabilization inciting interethnic discord, calling for violation of the constitutional order, holding illegal rallies… and much more." [19] IMAS's clients include the Prosecutor General's Office, the Ministry of Justice, and various local government administrations. [20]

Activists using social media are occasionally intercepted or punished, sometimes preemptively, by authorities who have prior knowledge of their planned activities. [21] Reports have emerged that authorities penetrated group chats on WhatsApp and Telegram, based on claims by activists that they faced repercussions for material they posted only on the communication apps. It is unclear how authorities could have gained

access to these closed chats, but it is generally understood that either there are informants in critical groups or police seize and access the phones of detained activists. [22]

During the coverage period, the government moved to introduce China-style video surveillance systems featuring facial recognition technology. [23] In September 2019, President Tokayev praised the technology he had observed on a recent visit to China, saying, “You click on a screen [where a person’s image is] and all the data comes up for that person, including literally everything: when he graduated from college, where he goes in his spare time, what kind of loans he has outstanding. We need to head in that direction.” [24] However, public criticism of a proposed “Smart CCTV” pilot in Almaty led to that project’s cancellation in January 2020. [25]

Amid the state of emergency brought on by the COVID-19 pandemic, authorities in Almaty, Kostanai, Nur-Sultan, and Oral required COVID-19 patients and quarantined individuals to install a geolocation-tracking app on their mobile devices so that their movements could be traced. [26]

In 2015, WikiLeaks published an exchange of emails between an alleged secret service official and Hacking Team, an Italian firm that sells surveillance software. The exchange suggests that the government might have obtained software to monitor and interfere with online traffic, including encrypted communications, as well as to perform targeted cyberattacks against certain users and devices. [27]

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**2** / 6

Telecommunications companies have fully implemented the new SORM technical regulations (see C5), effectively granting the Kazakhstani government real-time access to their subscribers’ data.

There is a process that governs authorities’ ability to request user data from various companies, but it is not always followed. Security agencies

can effectively access at will user data stored by the companies, as firms that wish to operate in the country have no means of resisting their demands. In its “exit report” upon leaving the Kazakhstani market, Tele2, the Swedish mobile service provider whose stake in Tele2-Altel was bought by Kazakhtelecom in 2019, noted that “it was not possible for Tele2 KZ to know how often the SORM system was used and whether the required warrant had been obtained.” [1]

Legislation obliges both fixed-line ISPs and mobile service providers to retain records of users’ online activities, phone numbers, billing details, IP addresses, browsing history, protocols of data transmission, and other data. [2] Providers must store user data for two years and grant access within 24 hours to “operative-investigatory bodies,” including the NSC and other security agencies, when approved by a prosecutor or “by coordination with the Prosecutor General's Office.” [3] The code of administrative offenses imposes fines on ISPs for failure to store user data. [4] Tele2’s exit report revealed that the company “started preparations to publish the number and nature of requests it receives from law enforcement to disclose historical (meta)data on customers’ usage of telecommunications services… but was not allowed [to] publish the data.” [5]

Domain names using the .kz country code must operate on domestic servers. [6] According to Kazakhstan’s laws on communications, informatization, and personal data and its protection, users’ personal data must be stored within the borders of Kazakhstan. [7] In late 2017, the government announced that it planned to negotiate with foreign social media platforms and persuade them to operate local servers that could provide easier state access to citizens’ personal data. [8] It was unclear whether negotiations had progressed at the time of writing.

Domestic website owners are required to retain commentators’ data for at least three months and provide the government with this information upon request. [9]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	**2** / 5

The coverage period featured an uptick in violence against activists and journalists working for online outlets. Adil Soz documented eight attacks against journalists in 2019 [1] and three in the first five months of 2020. [2]

In February 2020, DVK-affiliated activist Dulat Agadil died while in police custody shortly after being detained for allegedly violating the terms of his house arrest, which he had received for contempt of court. [3] Government officials, including President Tokayev, insisted that Agadil died of natural causes, and an official investigation concluded as much, [4] but other activists suspect that he was tortured, [5] with some maintaining that he was killed for his outspoken views. [6] Agadil maintained an active presence on social media platforms and was known for livestreaming protests. [7] As documented by the Coalition of Kazakhstani NGOs Against Torture, physical violence is a regular feature of law enforcement in the country. The group fielded 110 allegations of torture in 2019. [8]

During the coverage period, there were many cases of incidental violence against journalists during the dispersal of peaceful assemblies. In June 2019, amid antigovernment protests related to the presidential election, at least nine journalists who work online were briefly detained, and at least one was beaten by police. [9] Also in June 2019, Vlast.kz reporters were attacked in Shymkent while filming a protest staged by people evacuated from Arys after an explosion at an ammunition depot [10]; the next month, the reporters were threatened with arrest for trying to interview protesters in Almaty. [11] Also in July 2019, journalists for Azattyq.org, the Kazakh service of RFE/RL, were pepper-sprayed by an unidentified individual in Nur-Sultan [12] and physically attacked in Almaty. [13]

Members of the LGBT+ community in Kazakhstan frequently face online harassment. [14] In a July 2019 incident, a gay man in Nur-Sultan was reportedly catfished over VK and then tortured. [15]

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**1** / 3

Technical attacks against activists, dissidents, and independent media were observed during the coverage period, as were cyberattacks against public and private targets, including penetrations into government-owned information systems that resulted in citizens' personal data being leaked.

In July 2019, the Center for Analysis and Research of Cyberattacks (CARCA), a local cybersecurity association, reported that the personal data of 11 million citizens had been leaked from the Central Election Commission. [1] Law enforcement bodies launched an investigation into the incident in August 2019, but it was put on hold in January 2020 without explanation. [2] Also in July 2019, CARCA revealed that Damumed, a private medical information system used by many state and privately owned clinics, had been breached. [3] Officials and company representatives later confirmed the breach, blaming a nonspecific "human factor" and denying that Damumed was hacked. [4] In February 2020, CARCA reported on a vulnerability in the Prosecutor General's Office's information system that allowed citizens' personal data to be leaked; the vulnerability also allowed the unauthorized alteration of the data. [5] The government announced a plan to introduce a dedicated personal data protection agency in response to these incidents. [6]

Activists and dissidents were subjected to technical attacks prior to the coverage period, [7] and some expressed suspicions that the government was involved. [8] In September 2019, reports emerged that hackers working for the Chinese government had broken into telecoms networks to track Uighur travelers in Central Asia, including Kazakhstan. [9]

In November 2019, a Chinese cybersecurity firm reported on an extensive hacking operation in Kazakhstan by a group it dubbed "Golden Falcon" which apparently targeted government and military agencies, researchers, journalists, private companies, dissidents, and foreign diplomats. The

group, with alleged ties to Russia, had targeted Kazakhstan in the past, the firm said. Experts speculate that the operation may have been a Russia-sponsored advanced persistent threat actor, a Kazakh intelligence agency using Russian technical support, or a Russian mercenary group doing on-demand spying for the Kazakh government. [10]

On Kazakhstan

See all data, scores & information on this country or territory.

See More ›

Country Facts

Global Freedom Score

23 /100 **Not Free**

Internet Freedom Score

32 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2020

Other Years

2019

Be the first to know what's happening.

Email

Subscribe

Join the Freedom House monthly newsletter

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org