PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 114 (1544), 29 May 2020 © PISM

Surveillance in China during the COVID-19 Pandemic

Marcin Przychodniak

Surveillance of society is one of the main tools of power in China. The COVID-19 pandemic gave the government an excuse to intensify oversight, including through the solutions previously used mainly against Uighurs in Xinjiang. The effectiveness of surveillance is important to the Chinese authorities because of possible unrest arising from economic problems connected with COVID-19. The importance of surveillance in managing the virus in China has also led to demand in democratic countries to introduce similar practices.

Surveillance in China. Surveillance of society is an important tool for maintaining the monopoly of power of the Chinese Communist Party (CCP). The authorities present it as a guarantee of China's stability and development. It particularly focuses on people and groups that disagree publicly with the government's policy. These are dissidents (in 2019, the Nobel Prize winner Liu Xiaobo died after failing to receive medical treatment in a Chinese prison), NGOs working against the discrimination of, for example, Uighurs, Catholics, LGBT people, women, and independent lawyers representing these groups. Neither are party members, even at the highest level, immune from surveillance and the repression that follows. Surveillance of some officials has become an element of chairman Xi Jinping's fight with political opponents.

Since 2017, the testing ground for surveillance has been the special autonomous region of Xinjiang, where several methods (including Internet controls, personal monitoring and profiling, identification of location, collecting DNA and building big data systems) are used to identify Uighurs. They are accused by the authorities of terrorist activities and placed in special camps. Some solutions, such as mobile phone logins, were used to identify protestors in Hong Kong in 2019.

The body supervising the surveillance process is the political and legal committee of the CCP Central Committee. The general secretary of the committee is currently Chen Yixin. Until the end of April, he was also Xi`s special envoy for crisis management in Wuhan in connection with the epidemic.

Changes During COVID-19. The COVID-19 pandemic has served as a pretext for Chinese authorities to intensify surveillance, including the collection of sensitive data (fingerprints, medical histories, travel information and DNA samples) from a larger number of citizens. The authorities perceived the pandemic as a political threat related to the possible failure of the healthcare system in Wuhan and Hubei. The growing number of patients and deaths caused public dissatisfaction, expressed, among other places, via social media. Therefore, the authorities decided that it was necessary to increase control over the flow of information and public reactions, with Chen Yixin on guard.

The COVID-19 pandemic was also an excuse to test modern technological solutions previously used against Uighurs in the whole country (but primarily in Hubei). This meant, among other things, the installation of thousands of new cameras (there are already about 200 million in China), together with face recognition and profiling software. This year, an integrated national monitoring network of security cameras connected to big data systems is to be created. Chinese companies such as Cloud-Walk and Sense Time are developing artificial intelligence (AI) technologies that allow remote testing of body temperature and even racial

profiling. AI is also used in currently social credibility systems currently being tested. These systems are based on equivalents from the financial sector “rewarding” citizens with points for compliance with regulations. The long-term goal is for such systems to cover the whole country, giving the authorities the opportunity to shape preferred social behavior.

COVID-19 has also been a pretext for the development of mobile applications (produced on behalf of the province or city authorities), mandatory for citizens who want to travel or use public places. Often this was not possible without scanning QR codes. In contrast to sometimes inaccurate data from cellular triangulation, the authorities obtain the precise GPS location of citizens from common applications such as Alipay or WeChat. The most popular of these has been introduced in Hangzhou (and made obligatory across China). This is Alipay Global Health (about 700 million users), which organizes subscribers based on location and information on medical history and transmits data to police servers.

COVID-19 has facilitated the Chinese authorities’ access to information sent by users. Earlier, application owners such as Tencent and Alibaba were reluctant to share data due to consumer concerns and investors’ opinions (the companies are listed on the New York Stock Exchange). The activities of companies, however, remain dependent on party decisions, so they are forced to comply with the decisions of the authorities, especially in matters that the government considers to be political. This in turn facilitates surveillance of independent journalists, bloggers, and doctors who have been documenting the epidemic in Wuhan since December 2019 and allows the authorities to restrict their activities. The WeChat social network censors entries critical of Xi’s policy regarding COVID-19. Although the authorities, succumbing to social pressure and wanting to regulate the market, extended the regulations protecting users in 2017 in the Cybersecurity Act, the mobile applications commonly used during COVID-19 often were not covered by these regulations. In January and February, the Chinese people filed 2,000 complaints with the Cyberspace Office, of which around 15% were about software vulnerabilities.

The experience of surveillance of Uighurs and managing COVID-19 helped in the development of Chinese companies from the surveillance technology sector (including Huawei, Tencent, Hikvision and Dahua). Before the pandemic, they exported software and hardware to over 60 countries around the world, including Iran, Venezuela, Myanmar and Zimbabwe. They successfully competed with, for example, he Japanese NEC. This was aided by Chinese state banks’ loans to third countries for the purchase of Chinese equipment. COVID-19 has strengthened the position of Chinese companies as suppliers of equipment in Russia, but also in democratic countries. For example, Dahua thermal cameras have been bought by American companies such as Amazon, IBM and Chrysler. Both Hikvision and Dahua also operate in Denmark, providing elements of "smart cities" systems. Public administration bodies in the U.S. were banned in 2019 from doing business with these Chinese companies, on the grounds of their participation in the surveillance of the Uighurs.

Conclusions and Prospects. Surveillance is an immanent feature of China`s political system. According to the authorities, the expansion of its mechanisms based on AI will ultimately reduce government responsibility for uncomfortable decisions, making the systems and algorithms to blame for the repression of citizens. Surveillance solutions will also be wanted by the Chinese authorities in the context of possible unrest arising from the problems of the Chinese economy connected with COVID-19.

Monitoring, and above all the possible implementation of the tested social credibility systems, threatens the functioning of European companies (and their employees) in China. The EU should treat the exclusion of foreigners from these systems as a necessary condition for the finalisation of the EU-China Comprehensive Agreement on Investment.

In European debate, there is a belief in the effectiveness of surveillance in China’s management of COVID-19. This means that proposals for the implementation of similar mechanisms may appear in the manifestos of political parties and movements in EU countries (for example, in those such as Italy and Hungary, where China’s policy is an important element of the political debate). The use of Chinese practices and technologies would threaten EU citizens’ rights if they were implemented permanently and disproportionately. It is necessary, for example, to implement the ethical guidelines developed by the EC in 2019 regarding the use of AI in systems for assessing citizens’ behavior. In addition, the EU should seek to exclude Chinese companies involved in the surveillance of Chinese citizens from projects financed from European funds. The EU’s political pressure to cancel contracts with these entities should also apply to candidate countries such as Serbia and associate countries such as Ukraine.