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

POLICY PAPER

NO. 4 (217), JULY 2024 © PISM

Editors: Sławomir Dębski, Wojciech Lorenz

Threats Associated with China's Processing of Foreign Data Rising Fast

Marcin Przychodniak

The popularity of Chinese electronic devices, battery electric vehicles, and shopping and social media applications gives China access to large amounts of data. The Chinese authorities' control over the processing of this information means it could be used against the U.S. and the EU. It is in the interest of the EU and its Member States to raise awareness of the threat in societies and to strengthen regulations of Chinese actors within the single market.

Scale of the Threat

China accounts for more than 23% of international data flows, and the International Data Corporation estimates that by 2025 the country will control almost 28%, overtaking the current leader the U.S. One of the ways it has acquired this share is the activity of Chinese companies around the world—the operation of electronic devices (including for the Internet of Things), mobile phones, battery electric vehicles (BEVs), video surveillance equipment, and shopping, video conferencing, or social media applications. In most of these sectors, Chinese companies already hold the largest market share, thanks in part to lower prices made possible by state subsidies. Video surveillance equipment suppliers such as Dahua or Hikvision have a practical monopoly position in most of the Central European countries (e.g., Romania, Moldova, and Bulgaria). Chinese companies also supply AI-based surveillance technology (e.g., for profiling) to 67 countries worldwide (e.g., Germany, France, Italy, Romania, Mongolia, Russia, and the U.S.). In 13 EU member states, Chinese manufacturers' involvement in 4G infrastructure exceeds the level of 50%. In addition, data is acquired by China directly from the global network. The Australian Strategic Policy Institute and others identified a subsidiary of the Propaganda Department of the Central Committee (CC) called the Global Tone Communications company that processes more than 2 petabytes of data annually (equivalent to 20 billion social media photos; mainly relating to AI and facial-recognition technology) and subjects it to analysis for threats to China's security, as well as to use against the EU and the U.S.

These activities are used by China to gauge Western societies' views and influence them, including by shaping the debate on China.

These activities are used by China to gauge Western societies' views and influence them, including by shaping the debate on China. The processing of foreign data also provides an opportunity to share information and tools for its analysis with Russia, which can use it in its actions against the EU and NATO. It is possible for China to use the acquired data in hybrid operations (e.g., to influence electoral processes, including the U.S. elections this year), for disinformation or manipulation, or even to destabilise the socio-political situation (such as during the coronavirus pandemic). Threats from China also include critical infrastructure, for example, linking personal data to specific objects, such as employees of local military units. Systems and software operating Chinese cars, including BEVs, allow manufacturers to collect user location data and neighbourhood information. Big data sets are also being acquired by shopping apps (e.g., Shein or TEMU) and social media. The ability to learn about consumer preferences and suggest choices is applicable to products but can also be used to promote social or political messages with significant reach (TikTok has more than 170 million users in the U.S. alone and more than 140 million in the EU). The dangers of this were pointed out by, among others, Estonian and Norwegian intelligence in reports published in 2022. TikTok admitted that it had handed over data on U.S. journalists to its Chinese owner, ByteDance, as part of the company's investigation into information leaks, and it fired those responsible.

Tightening of Control by Chinese Authorities

In 2017, during a session on the importance of Big Data, the Politburo of the Communist Party of China (CPC) recognised that increasing the supervision of state and party organs over information processing is an important part of modernising China's economy. At the time, China's chairman Xi Jinping defined data as one of the factors of production, like capital, technology, or land, which must be subject to increased control by party institutions. Therefore, in recent years, the Chinese authorities have intensified their efforts to control the transfer of information from the private sector to the party and state institutions. Already in 2018, more than 90% of China's 500-largest private companies had CPC cells. Depending on the

Xi Jinping defined data as one of the factors of production, like capital, technology, or land, which must be subject to increased control by party institutions.

security importance of private companies, state institutions take a 1% stake in them (the so-called golden share). In 2021, this happened to ByteDance, the owner of TikTok.

The obligations of Chinese companies in the data-processing sphere are primarily set out in the Cybersecurity Law from 2017 (amended in 2018 and 2022). Its provisions in relation to Big Data were further developed by the 2021 Data Security Law. It defines the categories and ranks of information collected that affect national security and introduces financial penalties for refusing to provide it to state authorities. The Private Information Protection Act from 2021 is of a special nature. Under the guise of looking after users' rights, it introduced additional mechanisms for the oversight of technology companies by the Cyberspace Administration of China (CAC). This institution has been headed since 2018 by Zhuang Rongwen, who is also deputy head of the Central Committee's Propaganda Department. Party oversight of the CAC is provided by the Central Commission for Cyber Security and Information Technology under the Central Committee of the CCP, which is likely to be headed by Cai Qi, a trusted associate of Xi and member of the CCP Standing Committee, since August 2023. The authorities' oversight of Chinese companies is also strengthened by the 2020 "information processing technology" export regulations. These prohibit the sale of products to foreign companies without government approval. They apply to text analytics, voice recognition and content suggestion algorithms, and some others. These are often the most important technical solutions of a given company, as in the case of TikTok's unique recommendation algorithm responsible for the app's international success.

China is also seeking to increase its influence on global data protection regulation. In 2020, they proposed the Global Data Security Initiative, which was supported by Russia, among others, as reflected in statements following the Xi-Putin talks in 2022 and 2023. The text of the communiqué following their 2024 meeting no longer mentioned it by name, but pointed (as in previous years) to the two countries' cooperation on the Internet of Things and network and data security, including within the framework of the UN Working Group on Information Security (2021-2025). The Chinese initiative and cooperation with Russia were in response to the Clean Network programme announced by the Donald Trump administration in 2020. It was intended to activate cooperation between the U.S. and other democratic states in the face of Chinese threats to 5G and the digital sector, including the abandonment of Huawei's or ZTE's participation in building critical infrastructure.

EU and U.S. Actions

In the EU, the security sphere is the domain of the Member States. They are responsible for overseeing the EU's data protection regulations (GDPR). For violating them, for example, by illegally processing the data of minors, penalties have already been imposed on Chinese companies by Ireland and the Netherlands, among others. Some Member States (France, Sweden) have also taken measures to limit the participation of Chinese companies in the development of 5G infrastructure, in line with the EU's January 2020 recommendations, which some countries (Poland) have still not implemented in their legal orders. Restrictions on the use of Chinese surveillance cameras are also being introduced; Amsterdam, among others, introduced a ban on them in June this year. The Member States' solutions to Chinese data processing is therefore not strictly a security issue, but also is related to the position of such companies on the market, limiting the scale of their operations and opportunities for development, and in the case of internet applications and social media, also content moderation. In Poland, Shein and TEMU are being investigated by the Office of Competition and Consumer Protection (UOKiK) for unfair competition for not providing consumers with information as required by European law, among other allegations. In May this year, the Polish Ministry of Finance also announced fiscal inspections of these entities, although without specific information at that time.

The Member States' solutions to Chinese data processing is therefore not strictly a security issue, but also is related to the position of such companies on the market.

In July, the Ministry of Development and Technology announced cooperation with the EC in order to accelerate actions to force the platforms to act in accordance with European law. Indeed, the European Commission announced this month plans to abolish the €150 threshold exempting products imported from outside the EU, mainly via Chinese platforms, from duties.

The approach of the European Commission (EC) also focuses not only on security issues but also on the regulation of the operation of Chinese companies and on social issues. The regulation on foreign subsidies recently applied by the EC to the Chinese company Nuctech, a supplier of monitoring systems at airport terminals or border crossings, is one such instrument. Nuctech is accused of using a price advantage gained from subsidies to win tenders, including ones funded by the EU. In 2020, a study commissioned by the Canadian government reported that the company's X-ray scanners could collect and transmit information users' knowledge, including to China.

The EC also uses the Digital Services Act (DSA), which imposes obligations on companies operating sites with an active user base of more than 45 million, including effective content moderation (failure to comply can result in a penalty of up to 6% of a company's global turnover). In April this year, the EC initiated the procedure against Shein, in May against the PDD Group, the owner of the TEMU brand (which has more than 75 million users in the EU), and a year earlier against TikTok. This year, the EC also launched an investigation into TikTok's violations of the DSA in connection with a promotional programme launched in several EU countries that, by rewarding users for frequent use of the app, allegedly made children addicted to its use while increasing the amount of data collected. TikTok suspended the programme after the proceedings began. Under the Digital Market Act 2022 (DMA), the EC designated in September 2023 ByteDance, along with Amazon, Alphabet, and Meta, as "gatekeepers", obliging the firms to be transparent in their data protection mechanisms and not to abuse their dominant market position. TikTok and Meta have appealed this decision. In June this year, the Luxembourg court rejected TikTok's appeal, which still has the right of appeal to the EU Court of Justice. From 2023, there is also a ban in the EU on the use of this Chinese app on official devices of EP, EC, and European Council staff and a recommendation that they remove it from their private devices.

In the U.S., attempts to counter the threat of data processing by Chinese companies are being made at both the federal and state levels. Under the National Defence Authorisation Act, U.S. defence and critical infrastructure-related institutions are banned from using video surveillance equipment supplied by Huawei, Hytera, Hikvision, Dahua, and ZTE, among others. Some of these companies are also sanctioned by the U.S. for their involvement in the repression of Uighurs in Xinjiang. The Trump administration in December 2020 banned the use of TikTok by federal officials, albeit with a few exceptions (e.g., in situations involving national security, law enforcement, or security research). Bans on the use of the app by state officials and companies working with the administration are in place in more than 30 U.S. states. In 2020, the Trump administration tried by executive order to order the sale of TikTok by its Chinese owner, but this was first challenged in court and then revoked by President Joe Biden in 2021. However, in April this year. Congress passed, and President Biden signed, the Protecting Americans' Data from Hostile States Act (the states: China, North Korea, Russia, Iran), under which TikTok has nine months to sell a majority stake to an entity outside these countries or it will not be allowed to operate in the U.S. The company has challenged this decision in court citing, among other things, freedom of speech, which is likely to prolong the whole process. Officially, it has ruled out such a transaction, arguing, among other things, that the ban on the sale of algorithms imposed by the Chinese authorities does not allow it.

Restrictions in Other Countries and Organisations

In addition to the EU and the U.S., initiatives targeting Chinese data-processing companies are also being taken by others. In 2022, the UK and Australia banned the use of surveillance equipment

manufactured by HikVision or Dahua in government buildings. TikTok is also affected by the restrictions, and the motivation of some countries rooted in the inability of local authorities to oversee the operation of the app. In August 2023, TikTok was banned by Senegal, which demanded that the app block content supporting opposition leaders that the government believed was leading to destabilisation of the socio-political situation. India has banned the app twice, first in 2019 for a few days and then completely in 2020 with an order to remove the ability to download it to devices along with 58 other Chinese apps (including Shein and WeChat), as they were deemed a threat to state sovereignty. Restrictions are in place in Iran (as part of a censorship regime), Jordan (following the death of a police officer during riots in 2022 in which participants used the platform; the ban was imposed temporarily but remains in place today), Kyrgyzstan (since August 2023, as a threat to the development of minors), Nepal (since November 2023, on charges of social destabilisation), Taiwan (since December 2022, but only on devices belonging to members of the administration), Uzbekistan (from July 2022, due to violations of user data protection laws) and Kosovo (from June this year, on state administration official devices).

From March 2023, TikTok was also banned from being installed on NATO service devices. This was followed by similar restrictions in Alliance member states: Belgium, Denmark, Estonia, France (additionally, in May 2023, it was banned completely in New Caledonia as a counter-riot element), Latvia, the Netherlands, Norway, the UK, Canada, as well as NATO partners Australia and New Zealand, and neutral countries Austria, Ireland, and Malta.

Conclusions and Recommendations

With the increasing amount of foreign data processed by Chinese entities, control of this process by the Chinese authorities, and the growing realisation of their power ambitions, the threat of hostile use of the acquired information against the EU and the U.S. is increasing. Centralisation of the Chinese government by the CCP, the lack of an independent judiciary, and little transparency around these activities preclude the possibility of countering abuses by the data owners—other countries, companies, or individuals. This also differentiates Chinese actors from U.S. corporations, which do not infrequently obtain data in an equally aggressive manner and use similar algorithms, but do so primarily for business reasons. In democratic states, including the EU, there are also mechanisms in place to safeguard against their use for activities that are not in the interest of the Member States. The issues of data protection and access are already being addressed between the EU and the U.S. through the Trade and Technology Council. With the appointment of the new EC, the Council should continue its work, with data security issues one of its main areas of action. At the same time, stronger measures are needed in this context, mainly at the Member State level, to restrict data processing by Chinese entities.

Centralisation of the Chinese government by the CCP, the lack of an independent judiciary, and little transparency around these activities preclude the possibility of countering abuses by the data owners—other countries, companies, or individuals.

One new tool could be statutory regulations (or at least recommendations by the authorities) on restrictions on the movement of Chinese electric vehicles in the vicinity of government facilities and critical infrastructure, as well as access of other data-processing devices (e.g., within the framework of the Internet of Things) in sensitive areas from the point of view of national security. It is worth considering extending it to further areas (e.g., video surveillance) and using procedures for identifying "high-risk providers" introduced by the Member States when building 5G networks. The rationale for such actions could be the EU Data Act of December 2023, which in Article 23 obliges service providers (including Chinese companies) not to transmit data to third-country governments. Hence, it is crucial that some EU countries complete the alignment of their legislation with the 2020 EU standards, including Poland's finalisation of the amendment to its Cyber Security Law. A solution to limit the

possibility of manipulation of content and promotion of disinformation could be, as called for by NGOs, the development in the EU of platforms that give the user a choice of content recommendation systems (not included in the DSA). This would limit the operation of algorithms geared towards suggesting specific content to the viewer (rather than forcing the user to select it) and make it more difficult to possibly reach with a pro-China message. This also brings with it the need to strengthen education of the public on how digital corporations, including those from China, operate.

At the level of EU and NATO member states, the basic element is to ban the use of TikTok and other Chinese apps (or ones with data centres in China), such as Zoom, on devices belonging to public institutions. In Poland, there is only a recommendation from the Ministry of Digitalisation on this issue, but it is particularly relevant for entities operating in the area of defence and critical infrastructure.