EUROPEAN UNION
Institute for Security Studies

BRIEF / 21
Oct 2021

CHINA'S DATA STRATEGY

Creating a state-led market

by

Camille Boullenois
Project leader/Head of Brussels office at Sinolytics

INTRODUCTION

In 2019 and 2020, the European Union [1], the United Kingdom [2] and the United States [3] issued strategy papers on data governance acknowledging the importance of data to their economic development and national security. With different emphases, four competing objectives dominate these data strategies: innovation (using data to create new business models and boost economic growth); security (ensuring that sensitive data is not used by a hostile foreign power); privacy (protecting citizens from abusive use of personal data); and surveillance (using data to monitor and control citizens' and companies' behaviour).

In the past two years, China has been defining its own data strategy and governance regime and, while juggling the same four competing objectives as its Western counterparts, is taking an innovative approach. While the specific data governance framework is still being debated among scholars, policymakers, industrial lobbyists and state institutions, local pilot regulations on data and stakeholders' public positions have already hinted at its future characteristics.

This Brief aims to shed light on these debates over China's emerging data governance framework. It starts by describing the objectives of the framework,

Summary

- China's data strategy creates risks of abusive data collection on EU nationals and companies and challenges the European Union's strong emphasis on individual data rights. China's data governance framework also entails a risk of deepening data protectionism, where countries hold on to their data resources and do not share them with foreign actors.
- As for other 'factors of production', such as land, labour and capital, China has embarked on a process of carefully defining property rights for data; these rights depend on the type of stakeholder, the purpose of usage and a granular categorisation of data types.
- China's data governance framework, as discussed by policymakers and illustrated in local pilot schemes, emphasises corporate data rights and state-led data collection.

then summarises the debates around the new data rights that Chinese policymakers are establishing and analyses China's first local pilot regulations defining those rights. The Brief then focuses specifically on health data to illustrate how China's data governance regime is designed to work. Finally, the Brief gives an overview of the challenges that China's data governance framework presents for EU governments and companies. Ultimately, China's data governance regime will have important implications for the protection of EU citizens' data and creates a risk of data protectionism. It is therefore crucial that the EU understands early enough the direction that China is taking, so that it can respond appropriately.

China's data governance regime will have important implications for the protection of EU citizens' data.

UNLEASHING THE POTENTIAL OF DATA RESOURCES

As in many countries, the objectives of China's data governance policy have been evolving rapidly. Originally more concerned with data security and using data as a tool for surveillance and control, the Chinese government has in the past five years built a comprehensive data privacy protection regime and established a strategy to create a data market encouraging innovation and digital economic growth.

The Chinese government has long pursued a security-centred approach to data. Soon after the country opened up to the internet in the 1990s, the government took drastic steps to control access to the Net with its infamous 'Great Firewall'. In subsequent decades, protecting the country's cyber infrastructure and preventing cyberattacks and data leaks have become key goals of China's data governance system, with regulations such as the 2017 Cybersecurity Law and the 2021 Data Security Law.

Gaining an in-depth knowledge of its population for governance purposes has also long been part of the Chinese government's strategy. The digital policing 'Golden Shield' project, started in 1998 and operated by the Ministry of Public Security, included the establishment of a centralised criminal information system. A police data system known as the Integrated Joint Operations Platform later became infamous for its role in mass surveillance and human rights violations in Xinjiang.

The objective of protecting individuals' privacy, by comparison, made its appearance more recently. It was only in 2018 that China, following in the EU's footsteps and responding to citizens' concerns, started to put in place a systematic legal framework protecting data privacy, with the Personal Information Security Specification [4] (a revised version of which was released in 2020) and the flurry of personal information protection regulations that followed, culminating in the Personal Information Protection Law [5] issued in August 2021.

The push to develop the digital economy has also started to be integrated into China's data governance framework in the past five years. In 2015, the State Council issued the *Outline of Actions to Promote Big Data Development* [6], and the 13th five-year plan [7] issued in 2016 dedicated a whole chapter to the national big data development strategy. Encouraging the digital economy is important to the Chinese government for two reasons. First, China lags behind Western countries in smart manufacturing and industrial digitalisation. China, for instance, spends about six times less on IT as a proportion of gross domestic product (GDP) than the United States and three times less than Germany [8]. China's manufacturing is still largely low-tech, low-skilled and based on cheap labour, and data is seen as crucial to innovation and economic upgrading. Second, China's fast-growing e-commerce market is exceptionally strong, accounting for about 45 % of global transactions in that sector [9], and Chinese leaders want to capitalise on that strength.

To unleash the potential of data resources, the Chinese government has embarked on an unprecedented approach with regard to data governance. In October 2019, the Fourth Plenary Session of the 19th Central Committee of the Communist Party characterised data as a 'factor of production' [10]. This recognition paved the way for discussions about how to create a state-led data market, which would boost the digital economy by reducing transaction costs and allowing a smoother circulation of data. In 2020, an important State Council policy announced more market-oriented allocation of factors of production, including data [11].

Such a legal regime would have to balance the interests of three different stakeholders. Businesses, on one side of the triangle, are seeking easy collection of personal data; cheap, legal and fast access to databases with accurate data; and protection of their data from the government's reach. They also seek opportunities to exchange data with other businesses and to monetise data, low compliance costs for storing and using databases, and the right to analyse and use

data to enhance their business models. On another side of the triangle, individuals want restrictions on data collection to better protect their privacy, and they need guarantees that the data that companies and governments hold on them will not be used to harm or control them. On the third side of the triangle, various government agencies, as in many countries around the world, are pushing for increasing data collection on the population so that they can better oversee and control citizens' and companies' behaviour. Governments also seek to arbitrate between corporate and individuals' interests [12].

WHO WILL OWN CHINA'S DATA?

A data market, like other sectors of the Chinese economy, is understood in a very specific way: under China's 'socialist market economy' [13], the government has a significant role in defining rights and rules but recognises that letting players freely interact within this state-defined framework is most efficient. With this in mind, Chinese policymakers are now starting to call for a legal system that creates and defines data property rights, thus allowing data to become a tradable commodity that can be bought and sold on data trading platforms.

Creating a data ownership regime is controversial. Data has unique properties that make such an endeavour difficult: unlike tangible goods, data can be reproduced and disseminated at will. A creative and original effort, which is often the legal prerequisite for an object to be recognised as 'intellectual property', is not necessarily required to assemble a database. After years of heated discussions, the United States and the EU have not yet created such a data ownership regime. While proponents of the idea argue that it would create incentives to generate and share data, critics contend that it would stifle the growth of the digital economy, hinder the movement of data and accelerate data monopolisation (a process whereby a company acquires a dominant position across multiple sectors as a result of its capacity to hoard data on a very large scale) [14].

Chinese policymakers are now starting to call for a legal system that creates and defines data property rights.

The topic is also contentious within China. As it is a technical issue on which legislation is still in the early stages, there is room for public discussion and disagreement, which have been expressed openly in academic and news articles. But there has been, over the past two years, consistent and high-level support for introducing data property rights. The 14th five-year plan released in March 2021 – a high-level roadmap of the country's development covering 2021–2025 – called for 'establishing and improving data property rights transactions' [15]. The ninth meeting of the Central Finance and Economics Committee in March 2021 once again called for 'strengthening the construction of the data property rights system' [16].

Defining data ownership rights, according to proponents of this legislative effort, would have several benefits. It would encourage the circulation and sharing of data and help eliminate barriers to data usage. Companies would not be afraid to share data if they knew property over it was protected by law from appropriation and abusive copy. In addition, it would lead to a better distribution of wealth and benefits derived from data usage, by enabling the establishment of a taxation system based on data assets, for example. It could also break down natural data monopolies and ensure fair market competition by allowing smaller players to monetise their data rather than losing it, or to buy data they need from tech giants.

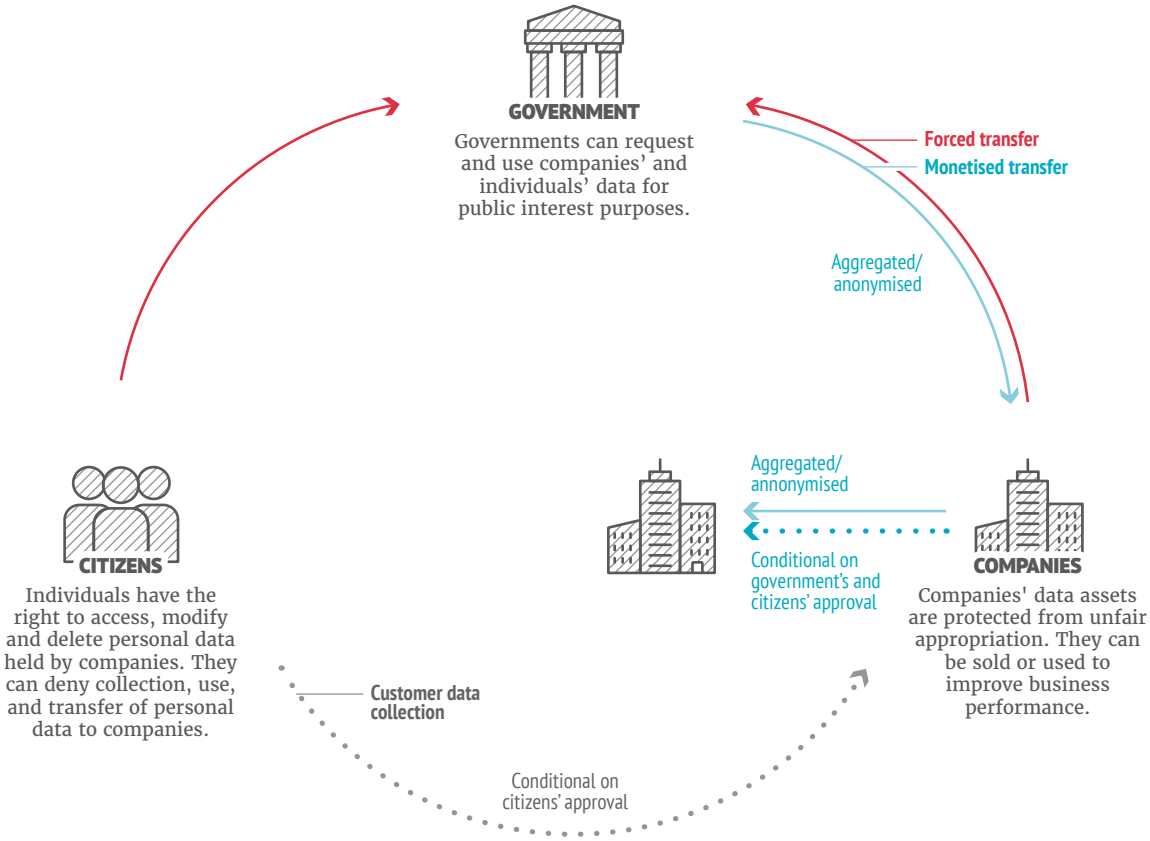
Although China's data ownership regime is still in its early stages, discussions among scholars, speeches by policymakers and local legislation hint at what it could look like. Most commentators agree that a data ownership regime should allow for non-exclusivity and multistakeholder joint ownership, with different data subjects and data processors exercising different rights over data according to their role in generating, maintaining and using it.

Under this framework, individuals have been granted substantive protection from harmful corporate data practices, with privacy provisions very similar to the EU's general data protection regulation (GDPR). But Chinese experts and policymakers also advocate a business-minded framework in which data ownership rights *sensu stricto* would be reserved to large databases held by businesses and not extended to individuals' personal data. This would mean that individuals would not be able to monetise or derive income from their personal information, but they would enjoy 'negative rights', for example the rights to refuse to grant authorisation to use their information, to delete it, to access it or to rectify it.

By contrast, enterprises collecting data would enjoy the rights to manage, use and derive income from the data they held – under certain conditions. One such condition is that the data collection either was authorised by the individuals that the data concerns (the data subjects) or responded to a limited set of necessary business purposes. Alternatively, businesses can freely use the data they have collected as

Circular transfers

Rights and transfers in China's emerging data governance regime between government, companies and citizens



long as it has been anonymised and can no longer be used to re-identify their data subjects.

Recent court cases such as *Weibo* v *Maimai* (2016) and *Tencent* v *Douyin* (2019) demonstrate that companies collecting and using large, anonymised data sets are already granted the right to protect them from unfair appropriation by other companies, even before China has enacted fully fledged legislation on this issue [17].

Nonetheless, Chinese policymakers have been careful not to endorse the monopolistic and unfair competition practices of China's tech giants and have recently embarked on a massive crackdown targeting them. Data resources, they argue, often form natural monopolies that need to be broken down to allow fairer market competition. Recent regulations thus strive to protect consumers from collective harms arising from data technologies. The Personal Information Protection Law, for instance, bans AI-powered differentiated pricing and allows data portability from one platform to the other, so as to avoid lock-in effects. A recent restructuring required of Ant Group, in April 2021, was another move in that direction: although the specific rules are still unclear, it is likely that the company will no longer be able to share data freely and opaquely between different industries and different subsidiaries of the group. Most recently, in September 2021, media reports indicated that Ant Group would be forced to create a separate loans app and to turn over user data to a new entity jointly owned by state companies [18].

The system of joint usage rights that would result from such rules is seen as a prerequisite for assetisation and monetisation of data sets. Since 2014, China has experimented with big data trading platforms for data transactions [19]. Furthermore, the proposition for a data property rights system put forward at the 2021 annual session of the National Committee of the Chinese People's Political Consultative Conference suggested the creation of a national data bank from which users could purchase data sets; the income incurred would be distributed among all stakeholders according to their participation in generating, collecting, maintaining and exploiting the data.

The ideas surrounding the creation of a data ownership regime in China also tend to envisage significant powers for the state as a key regulator and actor in data collection and sharing. Policymakers and experts are exploring different paths to encourage – or force – companies to grant the government access to their data resources, for example tax deduction policies for companies willing to share data or financial compensation for mandatory data sharing.

Equally important in these propositions, however, is the Chinese state opening its own data resources to the public. According to a statement by Chinese Premier Li Keqiang in 2016, more than 80 % of China's information and data resources are in the hands of government departments at all levels, but very little of this data is centralised, used or shared in a meaningful way[20]. The Chinese government wants to share some of this data with the public, but also to offer some for paid, conditional use by companies.

The last, but not least important, mission of the state is to protect national data resources, subject to fierce competition between countries. The Data Security Law released in June 2021 gives indications as to how these strategic resources will be protected. The law defines 'important data' that, if leaked, would be damaging to China's national security, public health, or economic and social development. This data would be subject to cumbersome export controls, including approval from local public security authorities.

All the ideas surrounding the creation of a data market have been synthesised in China's first draft local regulation defining data rights. This regulation, issued in Shenzhen in 2020 and revised in June 2021, will serve as a pilot and potentially a blueprint for a national definition of data rights, and it therefore offers invaluable insights into what China's data governance regime will look like in coming years[21].

The Shenzhen regulation defines three kinds of data rights for three types of actor: individuals, companies and the government. The personal data rights enjoyed by individuals obey a different logic from ownership rights – they are civil rights as defined in China's Civil Code. By comparison, companies enjoy rights closer to traditional ownership rights. They can buy and sell legally obtained data through legally established data trading platforms. The Shenzhen regulation also defines 'public data' as a 'new type of state-owned asset', held and collected by government authorities and public institutions such as those responsible for health, water supply, finance, telecommunications and transportation. Individuals and companies whose data is being collected by the state must comply, although they may raise objections if they believe the data collection is inaccurate or infringes on their personal privacy, business secrets or other legitimate interests. Some of this public data, then, is to be provided free of charge to the public, while some will be conditionally open or for state use only.

The Shenzhen regulation will serve as a pilot and potentially a blueprint for a national definition of data rights.

The Shenzhen regulation also provides for the establishment of a data transaction platform – which will construct data asset pricing indicators from multiple dimensions such as real time, time span, sample coverage, completeness, data type and level, and data mining potential – and for the setting up of 'data evaluation agencies' tasked with professionally assessing the value of data assets according to these indicators.

Finally, the regulation also outlines rules for international cross-border transfer and protection of strategic data resources. Although any transfer of personal information or important data must be reported to the local cyberspace authorities, the regulation leaves space for bilateral and multilateral cooperation mechanisms for free cross-border data circulation with other countries. A whitelist of countries, regions and international organisations with which cross-border flow of personal data is permitted will be released.

THE CASE OF HEALTH DATA

The case of medical data illustrates particularly well the complexity of establishing a data governance framework and the direction that the Chinese government is taking with regard to such a framework.

Medical data is especially sensitive when it comes to personal information, as it touches upon some of the most private and confidential pieces of information concerning individuals' lives. Regulations such as the Personal Information Protection Law qualify health data as sensitive and therefore strictly protected.

Medical data is also particularly valuable from a corporate perspective. Pharmaceutical companies, for example, crave access to large-scale data sets to develop and test new drugs, create personalised treatments and better target clients. China has acknowledged the potential of big data in developing the national health industry. In 2017, for instance, China planned the establishment of three national health big data industry groups, bringing together local governments, medical institutions and insurance companies[22].

Furthermore, medical data is crucial from both public health and national security perspectives. Most recently, the Chinese government saw the Covid-19 crisis as evidence of the importance of collecting detailed and granular data on citizens' health in case of health emergencies. In early 2020, Chinese cities started using a 'health code', which opened access to public buildings and transport[23]. So far, however, medical data integration and centralisation in China are far from the levels observed in Western European countries. This is mainly due to a lack of common

standards: different provinces, municipalities and hospitals have different ways of labelling and categorising medical information.

To incentivise the use of health data, China has started defining rights over medical data, tying them to very granular classifications of stakeholders, data types and situations. By defining the rights and responsibilities of every actor in a given situation and for a given category of data, the state hopes to establish a data regime that can both protect everybody's rights and encourage data usage.

The Chinese government saw the Covid-19 crisis as evidence of the importance of collecting granular data on citizens' health.

New guidelines on healthcare data security, which were passed in December 2020 and came into effect in July 2021, are meant to do just that [24]. They distinguish between standard personal health data and data obtained after basic de-identification processing – the latter can be used without individuals' authorisation for purposes of health research and education, public health, and medical care. Medical providers can rely on their own judgement to determine what personal health and medical data to use and disclose and are not obliged to agree to subjects' requests to restrict use of their data.

This provision is important, as it effectively gives strong, property-like rights to corporate actors as long as the data is used for certain purposes. It gives pharmaceutical companies more leeway to collect and use data for clinical trials: for post-market research or retrospective studies, for instance, the guidelines stipulate that no informed consent is needed provided the data has been through de-identification processing. This is crucial, as China is increasingly encouraging the use of 'real-world data' (data obtained throughout the life cycle of a drug or medical device) as evidence for the approval of new products.

Data rights attached to state institutions override other rights granted in the guidelines and no authorisation is needed from the data subject if data is collected for public health purposes. In practice, the government has started creating extensive lists of data that need to be collected for public health purposes. Regulations such as the national hospital data reporting management plan issued in 2019, for instance, list and standardise the data that health providers must submit to the National Health Commission [25].

The state also defines categories of health data that are especially protected from foreign collection and use. Human genetic resource data, which refers to information on genetic materials such as organs, tissues, cells, blood and DNA, is such a protected category: foreign institutions cannot collect human genetic resource data unless in partnership with Chinese institutions; strict rules define the role and responsibilities of the Chinese counterpart [26].

In other words, Chinese lawmakers are building a data governance regime in which the nature and roles of stakeholders, as well as the categories and purposes of data handling, play a part in determining their property rights. To better understand how this market would work, a fruitful comparison can be drawn between the data governance regime and China's land ownership regime. In both cases, multiple property rights coexist pertaining to the same object. In both cases, the nature of stakeholders (rural or urban, Chinese or foreign, individual or collective) defines the kind of rights they can claim on the object. Rural residents, for instance, have specific claims to land property that urban residents do not. For both data and land, rights also depend on specific purposes: some property rights in relation to land, for example, are restricted to it being used for agricultural purposes. This multifaceted ownership regime allows the government to balance the interests of different groups while maintaining overall control over important resources.

CHALLENGES FOR EUROPEAN GOVERNMENTS AND COMPANIES

The specificities of China's data governance regime have several important implications for European governments and companies.

A first set of challenges and risks arise from the Chinese government's propensity to collect and use data from individuals and companies. China is not unique in this respect: all governments do this to some extent. The EU's GDPR includes provisions allowing Member States to collect personal information in the public interest, if such collection is 'necessary and proportionate'. But China's debate around public ownership of data indicates that the government is willing to go well beyond such limited data collection. Massive amounts of data may be routinely obtained from individuals and companies and be used without much restriction based on a broad understanding of the 'public interest'.

This poses challenges to EU citizens in China, whose personal information may be abusively collected and used by the Chinese state. It also poses challenges

to companies, such as pharmaceutical and healthcare companies, that may be required to give away valuable or sensitive data to the Chinese government. Laws such as the National Security Law (2015), the Cybersecurity Law and the National Intelligence Law (2017) already give the central government sweeping powers to access foreign companies' sensitive data, including source code and intellectual property. Many companies report that routine data transfers to the Chinese government have increased over the past few years.

The Chinese strategy also poses a strategic and ideological challenge to the EU. In the triangle of stakeholders (businesses, government and individuals) presented earlier, the EU has so far strongly positioned itself on the side of individual rights, with the GDPR as a world-leading and world-shaping item of legislation. China's legislation, weighing rather on the business and government sides, might lead other countries to follow suit and put pressure on the EU's approach. Although China has adopted a personal information protection legal framework very similar to the EU's GDPR, the philosophy behind each approach is arguably different. While the EU is mostly concerned with human and consumer rights, China approaches personal information protection from a more holistic perspective, including economic growth and social stability as key factors. China's good performance in reining in the rise of Covid-19 infections, believed to be linked to massive collection and processing of individual data, could further influence other countries to follow suit. In September 2020, China unveiled its 'Global Initiative on Data Security', showing its ambition to set the global rules on data governance.

Beijing has extended state data protection to 'important data' deemed valuable for China's economic and social development.

A second set of challenges arises from China's data protectionism. While the EU has been very protective, from the outset, of citizens' personal information, Beijing has extended state data protection to 'important data' deemed valuable for China's economic and social development. Cross-border data transfer is likely to be subject to tit-for-tat strategies. The 2021 Data Security Law specifies, for example, that China will adopt 'corresponding measures' in its trading of data assets. In the context of growing tensions between China and the United States, recent data security investigations into Chinese companies following their initial public offering in the United States also hint at potential restrictions on overseas listing when sensitive data is at stake[27].

This creates a risk of deepening data protectionism, where countries hold on to their data resources and do not share them with foreign actors. More broadly, it would also endanger digital trade, as tech companies would have to operate within data islands instead of offering products across countries. This could have a heavy economic impact: data flows, valued at USD 7.8 trillion in 2014, were expected to nearly quadruple from 2017 levels by 2022[28].

POLICY RECOMMENDATIONS

For EU governments, there may be room to influence China's data legislation through bilateral and multilateral trade negotiations. The Personal Information Protection issued in August 2021 indicates that China will follow provisions on cross-border personal data transfer included in treaties or international agreements. The Regional Comprehensive Economic Partnership (RCEP) signed in November 2020 contains such provisions. China also recently signalled its desire to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, which stipulates that parties cannot require data localisation as a condition for conducting business, thus proving its willingness to negotiate on these issues.

Chinese local governments, although not autonomous from central government, could also constitute partners for discussion for both European governments and European companies, as they have started competing to attract investment in the local digital economy. The Hainan free trade zone, for instance, is experimenting with easier personal information transfer abroad and simplified procedures, along with physical infrastructure to facilitate quicker international data flows.

At this early stage in the debate, researchers, universities and government-run think tanks could fruitfully be involved in discussions around global data rules and norm-setting. For example, one crucial aspect of the protection of personal information is to certify that the data has been sufficiently anonymised. Although China has recently issued a standard on anonymisation processes, it is often impossible to define an *a priori* threshold beyond which anonymisation is sufficiently efficient. Without independent auditing, companies will do the bare minimum to avoid reducing the value of the data, incurring a higher risk of the data being re-identified if leaked. The EU has an important role to play in setting global rules in this respect.

More broadly, European governments and companies should closely follow the fast-evolving debates, legislation and law enforcement events surrounding China's data governance regime and monitor their potential impact on EU citizens and businesses.

References

[1] European Commission, *European Data Strategy*, February 2020 (https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en).

[2] UK Government, *National Data Strategy*, September 2020 (https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy).

[3] US Government, *Federal Data Strategy*, June 2019 (https://strategy.data.gov/).

[4] State Administration for Market Regulation and the National Standardization Administration, Information Security Technology – Personal Information Security Specification (信息安全技术个人信息安全规范), GB/T 35273-2020, March 2020 (http://pip.tc260.org.cn/assets/wz/2020-03-07/ef2dab88-cd9d-4748-814a-a3eca027beba.pdf).

[5] China National People's Congress, Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法), August 2021 (https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021).

[6] State Council, Notice of the State Council on issuing the action plan for promoting the development of big data (国务院关于印发促进大数据发展行动纲要的通知国发), August 2015 (http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm).

[7] Central Committee of the Communist Party of China and National Congress of the Chinese Communist Party, Outline of the 13th five-year plan for the national economic and social development of the People's Republic of China (中华人民共和国国民经济和社会发展第十三个五年规划纲要), March 2016 (http://www.xinhuanet.com/politics/2016lh/2016-03/17/c_1118366322.htm).

[8] Brinda, M. and Shin, M., 'How China's cloud market differs from others', Bain and Company, August 2019 (https://www.bain.com/insights/how-chinas-cloud-market-differs-from-others/).

[9] Kharas, H. and Dooley, M., 'The digital transformation of East Asian trade', *East Asia Forum*, Vol. 13, No 2, April–June 2021, pp. 14–16.

[10] Fourth Plenary Session of the 19th Central Committee of the Communist Party of China, *Decision of the Central Committee of the Communist Party of China on several major issues concerning upholding and improving the socialist system with Chinese characteristics and promoting the modernization of the national governance system and governance* (中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定), 31 October 2019 (http://www.12371.cn/2019/11/05/ARTI1572948516253457.shtml).

[11] State Council, *Opinions on building a more complete system and mechanism for the market-oriented allocation of factors* (关于构建更加完善的要素市场化配置体制机制的意见), 10 April 2019 (http://www.gov.cn/zhengce/2020-04/10/content_5500740.htm).

[12] Variants of this triangle have been proposed in various publications. See, for example, Deloitte Analytics, *Open Data – Driving growth, ingenuity and innovation*, 2012 (https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte-analytics/open-data-driving-growth-ingenuity-and-innovation.pdf).

[13] Xinhuanet, 'China to build high-level socialist market economy', 3 November 2020 (http://www.xinhuanet.com/english/2020-11/03/c_139488468.htm).

[14] Banterle, F., 'Data ownership in the data economy: a European dilemma', in Synodinou, T.E., Jougleux, P., Markou, C. and Prastitou, T. (eds), *EU Internet Law in the Digital Era*, Springer, Berlin, 2020, pp. 199–225 (https://doi.org/10.1007/978-3-030-25579-4_9).

[15] Central Committee of the Communist Party of China and National Congress of the Chinese Communist Party, 14th five-year plan for the national economic and social development of the People's Republic of China and the outline of long-term goals for 2035 (中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要), March 2021 (https://www.guancha.cn/politics/2021_03_13_583945.shtml).

[16] Xi Jinping's speech at the ninth meeting of the Central Finance and Economics Committee, 15 March 2021 (http://www.gov.cn/xinwen/2021-03/15/content_5593154.htm).

[17] In the first case, Weibo won after a court decided Maimai grabbed Weibo's user data without its authorization. In the second case, the court asked Douyin to stop sharing Wechat's user data with Duoshan, an app also owned by ByteDance. The legal battle is still ongoing, as Douyin said in May it would appeal an April 2021 court decision ordering it to pay 1.2 million US dollars to Tencent for violating its copyright.

[18] Yu, S. and McMorrow, R., 'Beijing to break up Ant's Alipay and force creation of separate loans app', *Financial Times*, 13 September 2021 (https://www.ft.com/content/01b7c7ca-71ad-4baa-bddf-a4d5e65c5d79).

[19] Zihou, W. and Xi, Y. (王子侯、杨曦), 'Big data transactions have spawned a huge underground industry chain, illegal collection and trafficking are rampant' (大数据交易催生庞大地下产业链 非法收集贩卖猖獗), *Economic Information Daily* (经济参考报), 25 August 2016 (http://finance.people.com.cn/n1/2016/0825/c1004-28663750.html).

[20] Min, G. (郭敏), 'Only when data is open and shared can its value be released' (数据只有开放共享 才能得到价值释放), DataYuan (数据猿), 3 September 2020 (http://www.datayuan.cn/article/17343.htm).

[21] Shenzhen Municipality, Shenzhen Special Economic Zone data regulation (draft for comment) (深圳经济特区数据条例, 征求意见稿), June 2021 (http://ifls.cupl.edu.cn/info/1066/1630.htm).

[22] Xinhuanet (新华网), 'Plan already determined: the "national team" led the establishment of three major health and medical big data groups' (格局已定 "国家队"主导筹建三大健康医疗大数据集团), 21 June 2017 (http://www.xinhuanet.com/2017-06/21/c_136383349.htm).

[23] Ee, S., 'We read the technical standards for China's "health code." Here's what we learned', Technode, 10 July 2020 (https://technode.com/2020/07/10/we-read-the-technical-standards-for-chinas-health-code-heres-what-we-learned/).

[24] National Information Security Standardization Technical Committee, Health and Medical Data Security Guidelines (GB/T 39725-2020) (健康医疗数据安全指南), March 2021 (https://www.shangyexinzhi.com/article/3421609.html).

[25] General Office of the National Health Commission, National hospital data reporting management plan (for trial implementation) (全国医院数据上报管理方案,试行), May 2019 (http://www.nhc.gov.cn/guihuaxxs/s10741/201905/e615f42ce0f346149dc74e4457099af6.shtml).

[26] State Council, Regulations of the People's Republic of China on the administration of human genetic resources (中华人民共和国人类遗传资源管理条例), May 2019 (http://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm).

[27] Ping, C. K. and Ng, S., 'China widens data-security probe of U.S.-listed tech companies', *Wall Street Journal*, 6 July 2021 (https://www.wsj.com/articles/chinese-unit-launches-review-into-u-s-listed-chinese-tech-companies-11625451374).

[28] Cisco, *Cisco Visual Networking Index: Forecast and trends, 2017–2022*, White Paper, November 2018. Cited in the World Bank's latest World Development Report, *Data for Better Lives*, 2021 (https://wdr2021.worldbank.org/).

Published by the EU Institute for Security Studies and printed in Belgium by Bietlot.
Cover image credit: Maxim Hopman/Unsplash

PRINT
ISBN 978-92-9462-031-6 CATALOGUE NUMBER QN-AK-21-021-EN-C ISSN 2599-8943 DOI 10.2815/32866
ONLINE
ISBN 978-92-9462-030-9 CATALOGUE NUMBER QN-AK-21-021-EN-N ISSN 2315-1110 DOI 10.2815/19300