7-2021

Data regulation with Chinese characteristics

Henry S. GAO
Singapore Management University, henrygao@smu.edu.sg

12

Data Regulation with Chinese Characteristics

*Henry S. Gao**

Across the Great Wall we can reach every corner in the world.
The first email sent from China on 20 September 1987.

A INTRODUCTION

The regulation of data has increasingly become a common feature of trade agreements. To understand this rule framework, it is essential to first identify the main players and interests at stake. In my view, data regulation in trade agreements mainly deals with three groups of interests, each corresponding to different stakeholders. The first is the commercial interests of the companies engaged in electronic commerce. Due to the unique nature of their business, most Internet companies need unhindered data flows to conduct their business. Thus, they demand free flow of information across the globe and oppose to data localization requirements. Behind the second group of interest is the person or the consumer, who supplies the raw data to use the services provided by the Internet companies. As both the raw data and the processed data are controlled by the companies, consumers, at least to the extent they would act in their best interest, wish to ensure that their privacy and personal data are properly protected. This is where the third, and arguably the strongest, stakeholder – the state – comes into play.

The state monitors and regulates the data used by the first two groups, which involves the collection, processing, access and transfer of data. In designing the regulatory framework, the state often tries to strike a balance between the different or

* Associate Professor of Law, Singapore Management University. Contact: henrygao@smu.edu.sg. This research has been supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of the National Research Foundation, Singapore.

even conflicting interests of the different players, by trying to ensure the protection of the privacy of personal data, while not unduly hindering the development of the economy. Faced with various threats, such as cyberwarfare and terrorism, the state also needs to ensure that public safety and national security are not compromised by rogue players roaming at large in cyberspace.

While all regulators would agree on the need to strike a balance between the clashing interests of different stakeholders, their approaches often differ in practice. Some jurisdictions prioritize the need to safeguard the privacy of their citizens. A good example in this regard is the General Data Protection Regulation (GDPR) of the European Union (EU), which recognizes '[t]he protection of natural persons in relation to the processing of personal data' as 'a fundamental right'.[1] On the other hand, some jurisdictions put the commercial interests of firms first. In the United States (US), this is reflected in the 1996 Telecommunication Act, which notes that it is 'the policy of the United States ... to preserve ... free market ... unfettered by Federal or State regulation'.[2] In contrast, national security concerns are often cited to justify restrictions on cross-border data flow, albeit in varying degrees in different countries. A recent example is China's 2017 Cybersecurity Law, which imposed several restrictions aiming to 'safeguard cyber security, protect cyberspace sovereignty and national security'.[3]

It is not easy to say which one is the best approach, as the various regulatory approaches often reflect the different legal, political, economic, social and cultural backgrounds of different countries. What is more important than passing judgement about different models, however, is to understand the inherent logic and mechanisms of the different regulatory regimes. In this chapter, I will focus on China, which is not only home to the largest e-commerce market in the world but also has one of the most tightly regulated cyberspaces. By providing a detailed analysis of the rationale and operation of 'data regulation with Chinese characteristics', the chapter seeks not only to help understand this discrete regulatory model but also to find ways to deal with such a regime at the international level.

B INTERNET REGULATION IN CHINA

The first email from China was reportedly sent on 20 September 1987 by a group of researchers at the Institute for Computer Science of China's State Commission of

[1] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L [2016] 119/1, at Recital 1.

[2] Telecommunication Act of 1996, 47 U.S.C. 230(b)(2).

[3] Article 1 Cybersecurity Law of the People's Republic of China [Zhonghua Renmin Gongheguo Wangluo Anquan Fa], adopted 7 November 2016, www.chinalawinfo.com.

Machine Industry to the University of Karlsruhe in Germany.[4] On 28 November 1990, China's national domain name – '.cn' – was registered by Professor Qian Tianbai, a pioneer in the Chinese Internet industry.[5] However, it was not until 20 April 1994 that the first connection to the international network was established by China Education and Research Network, which marked the launch of the Internet in China.[6] Since then, the Chinese Internet has grown by leaps and bounds, despite occasional hiccups, such as Google's exit from China in 2009.[7] In 2013, China's e-commerce volume exceeded 10 trillion RMB and China overtook the United States as the largest e-commerce market in the world.[8] Nowadays, Chinese e-commerce giants like Alibaba are among the biggest online retailers globally and Chinese online shopping festivals, such as the Singles Day (11.11) Sale have gained loyal followers all around the world.[9] In the latest race on the research and applications of big data, machine learning and artificial intelligence (AI), China is also quickly catching up with the United States, a world leader that increasingly sees its competitive edge being narrowed.[10]

Notwithstanding the phenomenal growth in the e-commerce sector, the Internet remains under tight regulation in China. The following section provides a detailed examination of this framework, paying specific attention to the regulation of data.

I *Overview of the Regulatory Landscape*

Just like the development of the Internet in China, the evolution of the regulatory landscape in China over the past twenty years is also a remarkable journey, where the haphazard regulatory patchwork was revamped in several iterations before culminating in one of the most sophisticated regulatory frameworks the world has

[4] Li W., 'In the Beginning . . .', *China Daily*, 17 March 2008.

[5] Ibid.

[6] State Council Information Office [Guowuyuan Xinwen Bangongshi], 'China's White Paper on the State of the Internet' [Zhongguo Hulianwang Zhuangkuang Baipishu], 8 June 2010.

[7] For a review of the background of the case and the trade law issues it raised, see H. S. Gao, 'Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS', *Asian Journal of WTO and International Health Law and Policy* 12 (2011), 347–385; H. S. Gao, 'Googling for the Trade-Human Rights Nexus in China: Can the WTO Help?', in M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2012), 247–275.

[8] Ministry of Finance of the People's Republic of China, 'China's Bulk E-Commerce Transaction Value Exceeds 10 Trillion' [Woguo Dazong Dianzi Shangwu Jiaoyie Yi Chao 10 Wanyi Yuan], *China Financial and Economic News* [Zhongguo Caijing Bao], 7 August 2014.

[9] See M. Smith, 'Australian Brands Woo Shoppers at China's Singles' Day Sales', *Financial Review*, 12 November 2018; J. Lim, 'Singles' Day Sales in S'pore Doubled from a Year Before: ShopBack's Data', *Today*, 12 November 2018.

[10] T. H. Davenport, 'China Is Catching up to the US on Artificial Intelligence Research', *The Conversation*, 27 February 2019.

ever seen. With the benefit of the hindsight, we can divide the development of the regulatory framework into four stages.

The initial stage was from 1987 to 1998, when the Internet was still in its embryonic stage and the government had yet to fully fathom its potential. Thus, the world wide web largely remained as the 'wild wide web' and untangled by regulations. This does not mean that there was no regulation at all during this period. To the contrary, two important regulations were introduced in the short span of one year – the 1996 Provisional Regulations on the Management of International Networking of Computer Information Networks[11] and the 1997 Measures for Security Protection Administration of the International Networking of Computer Information Networks.[12] Yet, the regulatory framework in this period suffered from the following weaknesses: First, these regulations were very low in the legislative hierarchy, as they were provisional regulations and administrative rules issued by the executive branch, which did not have the same force as national laws issued by the National People's Congress (NPC) and its Standing Committee. Moreover, these regulations were not made with the authorization of the legislature. Thus, at least in theory, these regulations could be challenged, especially with regards to provisions that contradicted the rules in legislations of a higher rank. Second, the regulatory framework was built in a piecemeal manner. There was no central agency coordinating the powers of the different agencies and no clear delineation of jurisdictions between the different agencies. This could potentially result in gaps as well as in overlaps in the regulatory framework, making the whole system rather inefficient. Third, these regulations all focused on the Internet hardware and there was no regulation on the software, not to mention content. Paradoxically, this contributed to the exponential growth of the Chinese cyberspace at the turn of the century, where people flocked in the pursuit of freedom of speech unavailable offline.

The second stage started with the establishment of the Ministry of Information Industry (MII) on 31 March 1998, which resulted from the merger of the Ministry of Posts and Telecommunications (MPT) and the Ministry of Electronic Industry (MEI).[13] With an explicit jurisdiction over the information industry, the MII became the main regulator of the Internet in China.[14] However, other agencies

[11] Provisional Regulations of the State Council on the Management of International Networking of Computer Information Networks [Jisuanji Xinxi Wangluo Guoji Lianwang Guanli Zanxing Guiding], Guowuyuan Ling No 195, 1 February 1996.

[12] Measures of the Ministry of Public Security for Security Protection Administration of the International Networking of Computer Information Networks [Jisuanji Xinxi Wangluo Guoji Lianwang Anquan Baohu Guanli Banfa], Gonganbu Ling No 33, 30 December 1997, available at www.chinalawinfo.com.

[13] Li Z., 'Institutional Reforms in These Years: The Ministry of Industry and Information Technology Changed Its Name to the Ministry of Information Industry in 2008 [Jigou Gaige Zhexienian: Gongxinbu 2008 Nian you Xinxi Chanyebu Gengming Erlai]', *The Economic Observer*, 1 March 2018.

[14] Ministry of Information Industry [Xinxi Chanyebu], 'Introduction on the Ministry of Information Industry [Xinxi Chanyebu Jianjie]', 21 September 2005.

quickly stepped into the cyberspace and started to compete with MII on the regulation of various issues such as online news, audio-visual services, online media and web security.[15] While these new agencies helped to fill the void in the regulatory space, their eagerness to capture more regulatory power also heightened the risk for potential turf wars. To address this, in 2001 the State Council re-established the National Informatization Leading Group.[16] Headed by then Premier Zhu Rongji, the Leading Group tried to coordinate among the different agencies. In November 2004, the General Office of the CCP Central Committee and the General Office of the State Council issued Opinions on Further Strengthening Internet Administration, which clearly divided the jurisdiction and responsibilities of all central government ministries and agencies involved in Internet governance.[17] However, as these agencies are all of the same ministerial rank, the problem of regulatory competition remained. This did not change until 2010, when the General Office of the CCP Central Committee and the General Office of the State Council issued Opinions on Strengthening and Improving Internet Administration.[18] Pursuant to the Opinions, the Cyberspace Administration of China (CAC) was established in 2011 as a ministerial-level agency.[19] While its main jurisdiction is content regulation, the CAC also presides over the troika of Internet governance, which includes, in addition to the CAC: the Ministry of Industry and Information Technology (MIIT), which inherited the portfolio of the MII; and the Ministry of Public Security (MPS), which is responsible for Internet crimes and safety issues.[20]

The third stage in the evolution of China's cyberspace regulation was heralded in 2013 by the Third Plenum Conference of the Eighteenth Party Congress, which

[15] Zhu W., 'Changes, Challenges and Modernization of Internet Governance in China [Zhongguo Hulianwang Jianguan de Bianqian, Tiaozhan, yu Xiandaihua]', *Journalism and Communication* [Xinwen yu Chuanbo Yanjiu], 7 (2014), 80–127, at 81.

[16] Wang Y., 'The Origin and Implications of the Central Leading Group on Cybersecurity and Informatisation [Zhongyang Wangluo Anquan yu Xinxihua Lingdao Xiaozu de Youlai Jiqi Yingxiang]', *People.cn* [Renminwang], 3 March 2014.

[17] The General Office of the CCP Central Committee and the General Office of the State Council, Opinions on Further Strengthening Internet Administration [Zhonggong Zhongyang Bangongting, Guowuyuan Bangongting Xiafale Guanyu Jinyibu Jiaqiang Hulianwang Guanli Gongzuo de Yijian], Zhongbanfa No 32 (2004), as cited in Hu L., 'Chinese Internet Legislation before 1998 [Yijiu Jiuba Nian Zhiqian de Zhongguo Hulianwang Lifa]', 7 March 2008, available at www.ideobook.com/375/internet-legislation-1998/.

[18] The General Office of the CCP Central Committee and the General Office of the State Council, Opinions on Strengthening and Improving Internet Administration [Zhonggong Zhongyang Bangongting, Guowuyuan Bangongting Xiafale Guanyu Jiaqiang he Gaijin Hulianwang Guanli Gongzuo de Yijian], Zhongbanfa No 24 (2010), as cited in Tu C., *Generality of Broadcasting Law* [Guangbo Dianshi Falv Zhidu Gailun] (Beijing: Communication University of China Publishing House, 2011), at 62.

[19] 'The State Council Office Announced the Establishment of the National Internet Information Office, Wang Chen Is Appointed as the Director [Guoban Tongzhi Sheli Guojia Hulianwang Xinxi Bangongshi, Wangchen Ren Zhuren]', *Xinhua Press*, 4 May 2011.

[20] Wang R., 'Internet Governance in China in Two Decades [Zhongguo Hulianwang Jianguan Ershi Nian]', Tencent Research Institute [Tengxun Yanjiuyuan], 4 December 2019.

adopted the Decision of the CCP Central Committee on Several Major Issues concerning Comprehensively Deepening Reform.[21] The Decision adopted the policy of 'positive adoption, scientific development, lawful administration and ensuring security' for the development of the Internet, and called for further strengthening of Internet governance, especially the further streamlining of its leadership system. Most notably, the Decision emphasized that the objective of Internet governance shall be ensuring 'the security of national Internet and information'. This was the first time that Internet governance was elevated to the level of national security in a major Party document, and it set the tone for a new era of China's Internet regulation.

In his report to the Third Plenum Meeting, President Xi covered eleven major issues, one of them being Internet governance.[22] He emphasized that Internet and information security is 'a matter of national security and social stability, and a new composite challenge facing China'.[23] Xi also noted that the existing Internet governance system was lagging behind the rapid development of Internet technology and applications, and suffered from problems such as duplication and overlapping of agencies and their jurisdictions, mismatch between power and responsibilities, and low efficiency. According to Xi, to further strengthen Chinese Internet governance, the functions of the relevant agencies needed to be reshuffled to provide a comprehensive governance framework that covered everything from technology to content, and from ensuring everyday security to combating crimes.

Pursuant to the Third Plenum Decision, the Central Leading Group on Cyber Security and Informatization was established in February 2014.[24] The Leading Group is the third 'super agency' established after the Third Plenum Meeting, with the other two in charge of the most important topics – comprehensively deepening reform and national security, respectively. With President Xi as its head and Premier Li Keqiang as the deputy, the Leading Group has twenty-two members, which include three of the seven members of the Politburo Standing Committee and nine of the twenty-five members of the Politburo. Eleven of its members are also members of the Leading Group on Comprehensively Deepening Reform, one is

[21] 'Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform [Zhonggong Zhongyang Guanyu Quanmian Shenhua Gaige Ruogan Zhongda Wenti de Jueding]', *Xinhua Press*, 15 November 2013.

[22] Xi J., 'Explanations of the Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform [Guanyu Zhonggong Zhongyang Guanyu Quanmian Shenhua Gaige Ruogan Zhongda Wenti de Jueding de Shuoming]', *cpcnews.cn*, 9 November 2013.

[23] Ibid.

[24] 'The Member List of the Central Leading Group on Cybersecurity and Informatization – Staffed by Twelve National-Leader Level Leaders with Overlappings with Leading Group on Comprehensively Deepening Reform [Zhongyang Wangluo Anquan he Xinxihua Lingdao Xiaozu Chengyuan Mingdan 12 Zhengfu Guoji Jianzhi Shengaizu]', *guancha.cn* [Guanchazhe], 28 February 2014.

Secretary-General of the State Council at Vice Premier level, while the rest are all heads of important ministries, including the all-powerful National Development and Reform Commission. Such high-level set-up signals that cyber security and informatization have been elevated to an unprecedented level and have now become important components of the overall national security strategy.[25] While the Leading Group remains an ad hoc body, it now has an office housed at the newly restructured Cyberspace Administration of China (CAC).[26] This greatly boosted the status of the CAC among the peer ministries, as it is one of the few agencies under direct leadership of President Xi. In August 2014, the State Council even delegated its power on cyberspace content regulation to the CAC.[27] This made the CAC the most powerful agency with regard to the regulation of the Internet, and particularly with regard to Internet content.

The emphasis on cyber security was further confirmed by the 2015 National Security Law, which considers cyber security as a key component of national security and directs the state to make the 'core technology of the Internet and information, key infrastructure and the information system and data in key areas secure and controllable' in order to 'protect national cyberspace security, safety and development'.[28] Moreover, Article 77 of the law requires all citizens and organizations to make timely reports on activities that endanger national security, truthfully provide evidence relating to such activities that one knows of, and provide the necessary support and assistance to national security agencies. If enforced strictly, the provision could be used to compel netizens to report 'harmful information' or activity in cyberspace, and throw China back to the days of the Cultural Revolution, where everyone was under the constant surveillance of each other. In practice, however, this clause has not yet been employed in such an aggressive manner by the authorities.

The evolution of China's Internet regulation finally culminated in the 2016 Cyber Security law, which emphasized in the first article that cybersecurity is a matter of cyber-sovereignty and national security. The heightened role of the CAC was also further cemented by Article 8 of the law, which entrusted it with the overall responsibility for the planning and coordination of cybersecurity work and relevant

[25] Ibid.

[26] 'National Internet Information Office Restructured, State Council Delegated the Power on Internet Content Administration and Enforcement [Guojia Wangxinban Chongzu Guowuyuan Shouquan Qi Fuze Hulianwang Neirong Guanli Zhifa]', *guancha.cn* [Guanchazhe], 28 August 2014.

[27] State Council, Notice on Delegation of Power on Administration of Internet Information Content to the National Internet Information Office [Guowuyuan Guanyu Shouquan Guojia Hulianwang Xinxi Bangongshi Fuze Hulianwang Xinxi Neirong Guanli Gongzuo de Tongzhi], Guofa No 33 (2014), 26 August 2014.

[28] Article 25 National Security Law of the People's Republic of China [Zhonghua Renmin Gongheguo Guojia Anquan Fa], as adopted at the Fifteenth Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on 1 July 2015, available at www.chinalawinfo.com.

supervision and administration, while the other ministries, such as the MII and MPS, are only responsible for the cybersecurity administration within their own jurisdictions.

II *China's Main Internet Regulations*

From early on, the Chinese government recognized the disruptive potential of the Internet and put it under strict regulation. For example, barely two years after China was connected to the Internet, the State Council issued the very first Internet regulation – the 1996 Provisional Regulations of the People's Republic of China on the Management of International Networking of Computer Information Networks ('Provisional Regulations').[29] According to Article 3, the Provisional Regulations apply to all international networking of computer information networks within China, which is defined as 'networking of the computer information networks inside the People's Republic of China and those in foreign countries with the purpose of international exchange of information'. The key provision is Article 6, which provides that 'computer information networks shall use the international entry and exit gateways provided by the Ministry of Posts and Telecommunications in the country's public telecommunications network when they carry out direct international networking. No units or individuals shall be allowed to establish or use other channels for international networking without authorization'.

Anyone found in violation of the provision could be punished with a fine up to 15,000 RMB,[30] which was a hefty amount in 1996. With merely seventeen articles, the Provisional Regulations seem rather rudimentary, especially considering the fact that it dealt with such a complicated subject matter as the Internet. However, upon closer examination, we can say that it actually encapsulated all three aspects of Chinese Internet regulations for the decades to come.

The first is hardware regulation, which mandates that all Internet connections must go through official gateways sanctioned by the Chinese government. Such regulation enables the Chinese government to effectively control Internet connection, especially in blocking and filtering certain international websites and services.

The second is software/applications regulation, which means that even the software for Internet access must be sanctioned by the government. This is indicated in Article 10 of the Provisional Regulations, which states that all individuals, legal persons and other organizations must connect to international networks through access networks, which in turn are required by Articles 6 and 8 to connect through the Internet, i.e., those international gateways sanctioned by the MPT. This requirement is made explicit in the Implementation Rules for the Provisional Regulations ('Implementation Rules') promulgated by the Leading Group for Information

[29] Ministry of Public Security, note 12.
[30] State Council, note 11, Article 14.

Technology Advancement under the State Council on 13 February 1998.[31] After repeating the requirement to use official international gateways and the prohibition on using other gateways in Article 7, the Implementation Rules went on to state in Article 10 that all access networks to international networks shall go through the Internet and international network connections through 'any other means' are explicitly prohibited. According to Article 3.3 of the Implementation Rules, the international entry and exit gateways are 'physical information channels used for international networking'. As Article 7 already explicitly prohibits the use of other physical gateways for connection, the interpretation of the law means that the term 'any other means' shall be interpreted broadly and includes other connection methods at both the hardware and software/applications levels. In other words, the term 'any other means' includes not only other physical gateways, but also ways to connect to the Internet through software such as virtual private network (VPN). This stringent requirement is repeated in Article 12 of the Implementation Rules, which further affirms that all individuals, legal persons and other organizations must connect to international networks through the access networks and not 'any other means'.

The third category of regulation regards content. Again here, the essential rule framework on content is already found in the Provisional Regulations, which states in Article 13 that 'the organizations and individuals conducting international networking businesses shall abide by relevant State laws and administrative decrees and strictly follow safety and security rules. They shall not use international networking for law-breaking or criminal activities that may endanger national security or divulge State secrets; or producing, consulting, duplicating or propagating information that may disturb social order or pornographic information'.

This strict regulation is also duly copied into Article 20 of Implementation Rules, with two small but significant twists. First, the subject of regulation expands from those conducting international networking businesses to the access units (Internet service providers, ISPs) and users. This makes sense, as the bulk of the content online is usually created by intermediaries and end users. Second, the same article also requires the three groups to immediately report any harmful information they discover to the relevant authorities and take effective measures to prevent the dissemination of such information. This is yet another important feature of Chinese Internet regulation that differs from other countries, especially the United States, which do not impose liabilities on ISPs pursuant to the 'safe harbour' rule. As we will see later, this approach has been extended to the regulation of data in recent years.

[31] Information Computerization Leaders Group of the State Council, Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China [Zhonghua Renmin Gongheguo Jisuanji Xinxi Wangluo Guoji Lianwang Guanli Zanxing Guiding Shishi Banfa], Guoxin No 001 (1998), 13 February 1998, available at www.chinalawinfo.com.

In the sections that follow, we examine the main Chinese Internet regulations along the three themes of hardware regulation, software regulation, and content/data regulation.

1 Hardware Regulation

According to Article 8 of the Implementation Rules, the nascent Internet in China is broken down into four networks: China Public Computer Network (CHINANET), China Golden Bridge Network (CHINAGBNET), China Education and Research Network (CERNET) and China Science and Technology Network (CSTNET), which are respectively administered by the MPT, the MEI, the State Education Commission, and Chinese Academy of Sciences. Among the four, the first two are commercial networks, while the last two are non-profit networks, which provide Internet services for the universities and research institutes under their respective jurisdictions. In 2000, China Mobile, the largest mobile company in China, also received approval to build an international Internet gateway.[32] To further regulate international gateways, the MPT issued Administrative Rules on International Networking Entry and Exit Gateways for Computer Information Networks,[33] which reiterated the prohibition on international networking through self-established international networking or other means including satellite.[34] The 2000 Telecommunication Regulation[35] also stated that all international telecommunication services shall go through the approved international gateways,[36] and explicitly prohibited operating international networking business through leasing dedicated international telecommunications lines, establishing relaying facilities without permission or other means.[37] To avoid confusion as to whether Internet services were part of telecommunication services, the Telecom Regulation also explicitly stated that both Internet connection service and Internet information service are part of value-added telecom services.[38]

When China acceded to the World Trade Organization (WTO) in 2001, the hardware restriction was also copied into its Schedule of Specific Commitments for Services, which notes that '[a]ll international telecommunications services shall go through gateways established with the approval of China's telecommunications

[32] Ministry of Information Industry, Approval of the Agreement to Form China Mobile Internet [Xinxi Chanyebu Guanyu Tongyi Zujian Zhongguo Yidong Hulianwang de Pifu], Xinbu Dian No 48 (2000), 17 January 2000, available at www.chinalawinfo.com.

[33] Ministry of Posts and Telecommunications, Notice on Issuing the Administrative Rules on International Networking Entry and Exit Gateways for Computer Information Networks [Guanyu Fabu Jisuanji Xinxi Wangluo Guoji Lianwang Churukou Xindao Guanli Banfa de Tongzhi], Youbu No 492 (1996), 9 April 1996.

[34] Ibid., Article 2.

[35] Telecommunication Regulation of the State Council of the People's Republic of China [Zhonghua Renmin Gongheguo Dianxin Tiaoli], Guowuyuan Ling No 291, 25 September 2000, available at www.chinalawinfo.com.

[36] Ibid., Article 65.

[37] Ibid., Article 59.1.

[38] Ibid., Appendix: Catalogue of Telecommunications Business.

authorities'.[39] There was considerable confusion as to whether China's commitments include Internet services. On the one hand, its commitments on value-added telecom services seem to include all the value-added telecom sub-sectors under the Services Sectoral Classification List – that is, h. Electronic mail; i. Voice mail; j. On-line information and database retrieval; k. Electronic data interchange; l. Enhanced/Value-added facsimile services (including store and forward, store and retrieve); m. Code and protocol conversion; n. Online information and/or data processing (including transaction processing). The only restriction seems to be that the services shall be provided through a joint venture with 50 per cent cap on foreign equity. On the other hand, China's Telecom Regulations list Internet connection services and Internet information services separately from the value-added telecom services listed earlier. One may argue that one of the value-added services listed in China's schedule – online information and/or data processing (including transaction processing) – has the CPC number 843**, which corresponds to online content services in the current CPC version.[40] However, a closer examination reveals that the correspondence is only superficial, as the two Internet services under the current CPC version correspond to 75231 and 75232 in the CPC provisional list ('CPCprov'),[41] which is the basis of Services Sectoral Classification List and thus for the GATS negotiations and commitments. Class 7523 is defined in CPCprov as 'data and message transmission services', which in turn can be broken into Subclass: 75231 – data network services, and Subclass: 75232 – electronic message and information services.[42] However, according to the explanatory notes, Class 7523 only covers the necessary network services (mostly the underlying hardware) for data transmission, rather than the provision of information online. Thus, at most, China's schedule would only cover Internet connection services but not Internet information services. However, even such an interpretation cannot get around the requirement to go through officially sanctioned international gateways, which is repeated ad nauseam in the regulations mentioned above and China's GATS schedule.

2 Software Regulation

As mentioned earlier, the Implementation Rules prohibits connection to international networks through 'any other means', which could include software designed to evade

[39] WTO Working Party on the Accession of China, Report of the Working Party on the Accession of China, Addendum: Schedule CLII – The People's Republic of China, Part II – Schedule of Specific Commitments on Services, WT/ACC/CHN/49/Add.2, adopted 1 October 2001, at footnote 3.

[40] United Nations Department of International Economic and Social Affairs, Statistics Division, Statistical Papers, 'Central Product Classification (CPC)', Series M No 77, Version 2.1, ST/ESA/STAT/SER.M/77/Ver.2.1 (2015).

[41] United Nations Department of International Economic and Social Affairs, Statistics Division, 'CPC Versions Correspondence Tables', available at https://unstats.un.org/unsd/classifications/Econ/tables/CPC/CPCv11_CPCprov/CPCv11_CPCprov.txt.

[42] For a more detailed analysis, see Gao, note 7, at 361–362.

official international gateways in addition to hardware. This is also copied into Article 59.1 of the Telecom Regulations, which prohibits the operation of international networking businesses through any means. The 1997 Measures for Security Protection Administration of the International Networking of Computer Information Networks provides further clarification by prohibiting unauthorized access to or use of computer information networks, which could cover access to international network using unauthorized software.[43]

After Google pulled out of China in 2009, the Chinese government continued to tighten its control on cyberspace and blocked the websites of major social media (Facebook, YouTube, Twitter, etc.) and major international media (Bloomberg, Reuters, New York Times, etc.). To access these websites, many netizens resorted to VPNs. In view of this, the MIIT issued a notice in 2017, which explicitly prohibited VPNs.[44] To minimize the impact on firms, MIIT later clarified that foreign trade firms and multinational corporations could still lease dedicated lines for international networking from authorized telecom operators.[45] However, according to MIIT, such private networks can only be used for the internal office needs of the firm, and cannot be used to connect data centres or platforms abroad to conduct telecom businesses, which means that the lines cannot be leased to private consumers who are not employees of such firms. Since then, China has launched a major campaign to crack down on VPNs, and people have been jailed[46] and fined for selling and using VPN services respectively.[47]

3 Content/Data Regulation

The main content regulation is the 2000 Administrative Measures on Internet Information Services,[48] which states in Article 15 that Internet Information Service Provider shall not produce, copy, distribute or disseminate information that is contrary to the basic principles laid down in the Constitution, laws or administration

[43] Ministry of Public Security, Measures for Security Protection Administration of the International Networking of Computer Information Networks [Jisuanji Xinxi Wangluo Guoji Lianwang Anquan Baohu Guanli Banfa], Gonganbu Ling No 33, 30 December 1997, available at www.chinalawinfo.com.

[44] Ministry of Industry and Information Technology, Notice of the Ministry of Industry and Information Technology on Clearing up and Regulating the Internet Access Services Market [Gongye he Xinxihuabu Guanyu Qingli Guifan Hulianwang Wangluo Jieru Fuwu Shichang de Tongzhi], Gongxinbu Xinguanhan No 32 (2017).

[45] 'The Ministry of Industry and Information Technology Responded to Internet Users' Questions Such as Using VPNs [Gongxinbu Huiying Wangmin VPN deng Shiyong Wenti]', *People.cn* [Renminwang], 24 January 2017.

[46] B. Haas, 'Man in China Sentenced to Five Years' Jail for Running VPN', *The Guardian*, 22 December 2017.

[47] C. Chen, 'Chinese VPN User Fined for Accessing Overseas Websites as Part of Beijing's Ongoing "Clean Up" of Internet', *South China Morning Post*, 7 January 2019.

[48] State Council, *Administrative* Measures on Internet Information Services [Hulianwang Xinxi Fuwu Guanli Banfa], Guowuyuan Ling No 292.

regulations; is seditious to the ruling regime of the state or the system of socialism; subverts state power or sabotages the unity of the state; incites ethnic hostility or racial discrimination, or disrupts racial unity; spreads rumours or disrupts social order; propagates feudal superstitions; disseminates obscenity, pornography or gambling; incites violence, murder or terror; instigates others to commit offences; publicly insults or defames others; harms the reputation or interests of the State; or has content prohibited by laws or administrative regulations.[49]

Apparently copied from the Telecom Regulations[50] and 1996 Interim Regulations on Electronic Publications,[51] the list has remained largely constant for the past twenty years. The only addition was made in 2002, when several regulations added a new category of 'harming the social morality or the excellent cultural traditions of the nationalities'.[52] This new category, however, seems to be restricted mainly to online publications and has not been incorporated into subsequent laws and regulations. For example, neither the Administrative Measures on Internet Information Services nor the Telecom Regulations added this new category in their 2011 and 2016 amendments. It is also worth noting that such stringent regulation is not restricted to the Internet sector, as other regulations in the same period share the same restrictions on content.[53]

One apparent gap in the 2000 Administrative Measures is that the rules apply only to Internet information service providers but not the users who generate such information. This gap was filled by the 1997 Measures for Security Protection

[49] The translation is taken from A. S. Y. Cheung, 'The Business of Governance – China's Legislation on Content Regulation in Cyberspace', *International Law and Politics* 38 (2005), 1–38, at 13–14.

[50] State Council, note 35, Article 57.

[51] General Administration of Press and Publication, Interim Regulations on Electronic Publications [Dianzi Chubanwu Guanli Zanxing Guiding], Xinwen Chubanshu Ling No 6, 14 March 1996, available at www.chinalawinfo.com.

[52] See, e.g., Article 17, Interim Provisions of the General Administration of Press and Publication, Ministry of Information Industry on the Administration of Internet Publication [Hulianwang Chuban Guanli Zanxing Guiding], 27 June 2002; Article 14, Regulations of the State Council on the Administration of Business Sites of Internet Access Services [Hulianwang Shangwang Fuwu Yingye Changsuo Guanli Tiaoli], Guowuyuan Ling No 363, 29 September 2002; See also Article 17, Interim Provisions of the Ministry of Culture on the Administration of Internet Culture [Hulianwang Wenhua Guanli Zanxing Guiding], Wenhuabu Ling No 27, 4 March 2003; Article 19 State Administration of Radio and Television, Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network [Hulianwang deng Xinxi Wangluo Chuanbo Shiting Jiemu Guanli Banfa], Guojia Guangbo Dianying Dianshi Zongju Ling No 39, 6 July 2004, available at www.chinalawinfo.com.

[53] See Regulations of the State Council of the People's Republic of China on the Administration of Audio-Visual Products [Zhonghua Renmin Gongheguo Yinxiang Zhipin Guanli Tiaoli], Guowuyuan Ling No 165, 1 October 1994; State Council, Regulations on Administration of Films [Dianying Guanli Tiaoli], Guowuyuan Ling No 200, 1 July 1996; Regulations of the State Council on Broadcasting and Television Administration [Guangbo Dianshi Guanli Tiaoli], Guowuyuan Ling No 228, 1 September 1997, available at www.chinalawinfo.com.

Administration of the International Networking of Computer Information Networks, which expands the liability to 'any organization or individual'.[54] In judicial practice, the offense of 'Picking Quarrels and Provoking Trouble' has also been invoked on a case-by-case basis against people posting information online about various social problems. One example is the case of Zhao Lianhai, who was jailed for two-and-half years for trying to collect information about contaminated milk with a self-built website.[55] In 2013, the practice was further institutionalized when the Supreme People's Court and Supreme People's Procuratorate jointly issued a judicial interpretation, which clarifies that posting defamatory information online would be subject to the offence of criminal defamation under Article 246 of the Chinese Penal Code.[56] Moreover, in recognition of the special nature of online information dissemination, the judicial interpretation also states that the defamation would be considered to be 'serious', if the information is clicked or browsed more than 5,000 times or forwarded more than 500 times.[57] In 2015, the Penal Code was also amended to add an additional clause in Article 291, which makes it an offence to fabricate information about natural disasters or crime and spread them online, or to spread such false information knowingly online. The issue was finally sealed when the new 2017 Cyber Security Law expanded the liability for prohibited online content from organizations to individuals, which was repeated in two separate provisions (Articles 12 and 48).

One could argue that such draconian laws on netizens are rather unnecessary, especially considering the fact that, unlike the United States, the Internet information service providers are directly liable for the contents generated by users. Under the 2000 Administrative Measures, for example, the Internet information service providers are required, upon discovering prohibited information on their website, to stop the transmission, keep relevant records, and report to the relevant state authorities.[58] To give real teeth to the requirement, Article 23 of the Administrative Measures also stipulates that Internet information service providers found in violation could have their licences revoked and websites shut down.[59]

The liability for Internet information service providers was duly copied in the Cybersecurity Law.[60] Moreover, it went one step further by requiring Internet

[54] Ministry of Public Security, note 12, Article 5.

[55] B. Blanchard, 'China Court Sentences Melamine Milk Activist to Jail', *Reuters*, 10 November 2010.

[56] Supreme People's Court and the Supreme People's Procuratorate, Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in Handling Defamation and Other Criminal Cases through Information Networks [Zuigao Renmin Fayuan, Zuigao Renmin Jianchayuan Guanyu Banli Liyong Xinxi Wangluo Shishi Feibang Deng Xingshi Anjian Shiyong Falv Ruogan Wenti de Jieshi], Fa Shi No 21 (2013), 5 September 2013.

[57] Ibid., Article 2.

[58] State Council, note 48, Article 16.

[59] Ibid., Article 23.

[60] Cybersecurity Law, note 3, Article 47.

information service providers to establish mechanism to facilitate online complaints and reports.[61] A dedicated hotline and website (www.12377.cn) were also set up to handle reports on 'illegal and unhealthy information', with the first category being 'political information'.[62] In 2018 and 2019, between ten million and thirty million reports were made on average every month, with the majority being directed against major social media sites, such as Weibo, Tencent and search engines, such as Baidu.[63]

Another innovation in the Cybersecurity Law is the shift from the regulation of content to requirements on where such content, or data, shall be stored. According to Article 37, operators of critical information infrastructure are required to locally store personal information and important data collected and generated in their operations within China. If they need to send such data abroad due to business necessity, they have to first undergo security assessment by the authorities. This provision raised several concerns. First is what constitutes 'critical information infrastructure'. Article 31 defines this as infrastructure in 'important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs', as well as such 'that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage'. Such a broad definition could potentially capture everything and is not really helpful nor does it give much guidance, which is why the same article also directs the State Council to develop the 'specific scope of critical information infrastructure'.

In 2016, the CAC issued the National Network Security Inspection Operation Manual[64] and the Guide on the Determination of Critical Information Infrastructure,[65] which clarified the scope of critical information infrastructure by grouping them into three categories: (i) websites, which includes websites of

[61] Ibid., Article 49.

[62] Cyberspace Administration of China (National Internet Information Office), the Center for Reporting Illegal and Bad Information [Zhongyang Wangxinban (Guojia Hulianwang Xinxi Bangongshi) Weifa he Buliang Xinxi Jvbao Zhongxin].

[63] Cyberspace Administration of China (National Internet Information Office), the Center for Reporting Illegal and Bad Information [Zhongyang Wangxinban (Guojia Hulianwang Xinxi Bangongshi) Weifa he Buliang Xinxi Jvbao Zhongxin], Acceptance of National Network Reporting in June 2019 [2019 Nian 6 Yue Quanguo Wangluo Jvbao Shouli Qingkuang], 3 July 2019.

[64] Central Leading Group on Cyber Security and Informatisation General Office, Network Security Coordination Bureau, National Network Security Inspection Operation Manual [Guojia Wangluo Anquan Jiancha Caozuo Zhinan], June 2016.

[65] Guide on the Determination of Critical Information Infrastructure (Trial) [Guanjian Xinxi Jichu Sheshi Queding Zhinan (Shixing)], in Notice on Conducting Network Security Inspections of Key Information Infrastructure [Guanyu Kaizhan Guanjian Xinxi Jichu Sheshi Wangluo Anquan Jiancha de Tongzhi], Zhongwangban Fawen No 3 (2006), Annex 1, July 2016.

government and party organizations, enterprises and public institutions, and news media; (ii) platforms, which include Internet service platforms for instant messaging, online shopping, online payment, search engines, emails, online forum, maps, and audio video; and (iii) production operations, which include office and business systems, industrial control systems, big data centres, cloud computing and TV broadcasting systems.

The CAC also laid down three steps in determining the critical information infrastructure, which starts with the identification of the critical operation, then continues with the determination of the information system or industrial control system supporting such critical operation, and concludes with the final determination based on the level of the critical operations' reliance on such systems and possible damages resulting from security breaches in these systems. More specifically, they listed eleven sectors, which include energy, finance, transportation, hydraulics, medical, environmental protection, industrial manufacturing, utilities, telecom and Internet, radio and TV, and government agencies. The detailed criteria are both quantitative and qualitative. For example, on the one hand, critical information infrastructure includes websites with daily visitor counts of more than one million people and platforms with more than ten million registered users or more than one million daily active users, or daily transaction value of ten million RMB. On the other hand, even those that do not meet the quantitative criterion could be deemed to be critical information infrastructure if there are risks of security breaches that would lead to leakage of sensitive information about firms or enterprises, or leakage of fundamental national data on geology, population and resources, or seriously harming the image of the government or social order, or national security. The potentially wide reach of the criteria was well illustrated by the case of the BGI Group, which was fined by the Ministry of Science and Technology in October 2018 for exporting certain human genome information abroad via the Internet without authorization.[66] Given the nature of their business, the BGI case could fall under the category of 'leakage of fundamental national data on … population', as mentioned earlier.

4 Summary

From the discussion on the remarkable evolution of Internet regulation in China over the past twenty-five years, we can distil two key trends: First, in terms of the institutional framework, we have seen the development from the period of no man's land in the 1990s to the period of proliferation of regulation and regulators with overlapping and competing jurisdictions in the first decade of the new century. Since the beginning of the current decade, however, we have seen the power of Internet regulation consolidated under the CAC, which emerged as the dominating agency presiding over the troika of Internet governance, with the MIIT and MPS

[66] An S., 'How to Conduct "Safety Check" for Exporting Data' [Shuju Chujing Ruhe 'Anjian'], *zhihu*, available at https://zhuanlan.zhihu.com/p/65413452.

playing supporting roles. Second, in terms of the substantive regulations, we have not only seen the initial gaps in the regulatory landscape being filled with more and more detailed regulation, but also the shift in the regulatory focus. At first, the regulations focused on the technology, or the hardware of the Internet. Gradually, however, the focus shifted to the software, and then to the content, and now even to the data. This moves the regulations closer and closer to the heart of the matter, as the Internet, at the end of the day, is nothing but strings of zeros and ones arranged in specific sequences. With the adoption of the Cybersecurity Law in 2016, the focus has now been shifted to security, as the Internet is increasingly regarded as the key challenge to the all-powerful control of the Party. Thus, for China, Internet or data regulation has been presently elevated to a matter of national security. To put it in the words of President Xi, 'there is no national security without cybersecurity'.[67] Moreover, he even linked the survival of the Party with the Internet, by solemnly warning in 2013 that 'unless we solve the challenge of the Internet, the Party cannot stay in power indefinitely'.[68] The key to understand data regulation in China, therefore, must be 'security'. The heightened link with security not only explains the domestic regulatory framework in China but also informs how China would deal with the issue at the international level.

C TRADE AGREEMENTS

Ever since the Declaration on Global Electronic Commerce at the Second WTO Ministerial Conference in May 1998, WTO members have been exploring ways to incorporate Internet and data regulation into trade agreements.[69] While not much success was made in the WTO collectively, individual members were able to address the issue in other fora such as free trade agreements (FTAs) and the plurilateral Trade in Services Agreement (TiSA) initiative.[70] It makes good sense to address the issue in international trade agreements, as the Internet was born with an international nature and closely linked to commerce. At the same time, however, a country's position on Internet and data regulation in trade agreements is often heavily influenced by its domestic regulatory approach, and China is no exception.

In a way, China's first encounter with data regulation in the WTO started on the wrong foot as it concerned a sensitive area: China's regulation of publications and

[67] 'The Central Leading Group on Cyber Security and Informatisation Held Its First Meeting [Zhongyang Wangluo Anquan he Xinxihua Lingdao Xiaozu Diyici Huiyi Zhaokai]', *Xinhua Press*, 27 February 2014.

[68] Xi J., 'Speech at the National Propaganda and Thought Work Conference [Zai Quanguo Xuanchuan Sixiang Gongzuo Huiyi shang de Jianghua]', 19 August 2013, as cited in Z. Hanhua, 'Xi Jinping Hulianwang Fazhi Sixiang Yanjiu [Study on Xi Jinping's Thoughts on Internet Legal Governance]', *China Legal Science* [Zhongguo Faxue] 3 (2017), at 7.

[69] For an overview of the issues, see H. S. Gao, 'Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation', *Legal Issues of Economic Integration* 45 (2018), 47–70.

[70] Ibid.

audio-visual products.[71] In the case, the United States complained that China has failed to grant foreign firms the right to import and distribute publication and audio-visual products. One of the key issues in the case was whether China's commitments on 'sound recording distribution services' cover 'electronic distribution of sound recordings', as alleged by the United States.[72] China disagreed with the US approach and argued instead that such electronic distribution 'in fact corresponds to network music services',[73] which only emerged in 2001 and were completely different in kind from the 'sound recording distribution services'. According to China, the most fundamental difference between the two is that, unlike 'traditional' sound recording distribution services, network music services 'do not supply the users with sound recordings in physical form, but supply them with the right to use a musical content'.[74] In response, the United States cited the panel's statement *in US – Gambling*[75] that 'the GATS does not limit the various technologically possible means of delivery under mode 1', as well as the principle of 'technological neutrality' mentioned in the Work Programme on Electronic Commerce – Progress Report to the General Council,[76] and argued that electronic distribution is merely a means of delivery rather than a new type of service.[77] Furthermore, the United States argued that the term 'distribution' encompasses not only the distribution of goods, but also distribution of services.[78] After a lengthy discussion covering the ordinary meaning, the context, the provisions of the GATS, the object and purpose and various supplementary means of interpretation, the panel concluded that the term 'sound recording distribution services' does extend to distribution of sound recording through electronic means.[79] China appealed the panel's findings, but they were upheld by the Appellate Body, which largely adopted the panel's reasoning.[80]

The case was also the first WTO case concerning China's censorship regime. It is interesting to note, however, that the United States did not challenge the censorship

[71] Panel Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China – Publications and Audiovisual Products)*, WT/DS363/R and Corr.1, adopted 19 January 2010, as modified by Appellate Body Report WT/DS363/AB/R.

[72] Ibid., at paras. 4.49–4.71.

[73] Ibid., at para. 4.147.

[74] Ibid., at para. 4.149.

[75] Panel Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R, adopted 20 April 2005, as modified by Appellate Body Report WT/DS285/AB/R.

[76] WTO, Work Programme on Electronic Commerce, Progress Report to the General Council, S/L/74 (1999), at para. 4.

[77] *China – Publications and Audiovisual Products*, note 71, at para. 4.69.

[78] Ibid., at para. 7.1156.

[79] Ibid., at paras. 7.1168–7.1265.

[80] Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China – Publications and Audiovisual Products)*, WT/DS363/AB/R, adopted 19 January 2010, at paras. 338–413.

regime per se.[81] Instead, the United States only challenged the alleged discrimination in the operation of the regime, where imported products were subject to more burdensome content review requirements.[82] Ironically, the United States even proposed, as the solution to the alleged discrimination, that the Chinese Government itself shall shoulder the sole responsibility for conducting content review, rather than outsourcing it to importing firms.[83]

With such an unpleasant experience, China took a cautious approach on the inclusion of Internet or data regulation in other trade fora. While it has signed more than a dozen FTAs so far, most of them have not included provisions on such regulations. The only exceptions are the two FTAs China signed with South Korea and Australia[84] in 2015 and the amendment of the FTA signed with Chile in 2018, which include stand-alone chapters on e-commerce. However, unlike the US FTAs, which often include provisions on free flow of data and ban on data localization requirements,[85] the earlier mentioned FTAs only address e-commerce-related issues, such as the moratorium on customs duties on electronic transmissions; electronic authentication and electronic signatures; protection of personal information in e-commerce; and paperless trading.[86] Thus, they do not really address Internet and data regulation issues as such.

A similar approach is taken by China in the WTO negotiations. Even though the United States has long been calling for rules on issues such as free cross-border data flow and ban on data localization requirements, China has ignored these issues until very recently. For example, in its communication on e-commerce jointly tabled with Pakistan before the Eleventh Ministerial Conference, China focused only on 'cross-border trade in goods enabled by Internet, together with services directly supporting such trade in goods, such as payment and logistics services'.[87] As I have mentioned in another article, this approach is a reflection of the nature of business of most Chinese Internet firms, as they tend to focus on trade in physical goods facilitated by the Internet, rather than digital products like Google and Netflix.[88] Thus, when over

[81] Ibid., at para. 20.
[82] *China – Publications and Audiovisual Products*, note 71, at paras. 4.72–4.85.
[83] *China – Publications and Audiovisual Products*, note 71, at para. 7.875; *China – Publications and Audiovisual Products*, note 80, at para. 72.
[84] See also H. S. Gao, 'E-Commerce in ChAFTA: New Wine in Old Wineskins?', in C. Piker, H. Wang, and W. Zhou (eds), *The China Australia Free Trade Agreement: A Twenty-first-Century Model*, (Oxford: Hart Publishing, 2018), 283–303.
[85] See Gao, note 69.
[86] See H. S. Gao, 'Digital or Trade? The Contrasting Approaches of China and US to Digital Trade', *Journal of International Economic Law* 21 (2018), 297–321.
[87] WTO General Council, Council for Trade in Goods, Council for Trade in Services, Committee on Trade and Development, Work Programme on Electronic Commerce: Aiming at the Eleventh Ministerial Conference, Communication from the People's Republic of China and Pakistan, Revision, JOB/GC/110/Rev.1, JOB/CTG/2/Rev.1, JOB/SERV/243/Rev.1, JOB/DEV/39/Rev.1 (2016).
[88] See Gao, note 86.

seventy WTO members issued a joint statement on launching the negotiations on e-commerce at the Eleventh Ministerial Conference in December 2017,[89] China declined to join. When these members decided to formally launch the e-commerce negotiations in January 2019, however, China changed its position and jumped on the negotiation.[90] In April 2019, China issued a communication on the joint statement negotiation, in which it repeated the focus on cross-border trade in goods enabled by the Internet.[91] At the same time, however, it also addressed the main concerns of the United States, including data flows, data storage and treatment of digital products, in the following manner.

First, rather than ignoring these issues as it has done in the past, China chose to face them and acknowledge them as issues of concern for some members. This itself is a positive sign, as it indicates China's willingness to engage on these issues. Second, at the same time, China also indicated that it was not ready to discuss these issues, at least not in the early stages of the negotiation. Citing the 'complexity and sensitivity' of these issues, as well as 'the vastly divergent views among the Members', China stated that 'more exploratory discussions are needed before bringing such issues to the WTO negotiation, so as to allow Members to fully understand their implications and impacts, as well as related challenges and opportunities'.[92] Such approach is all too familiar to those who follow WTO negotiations closely, as it is basically a polite way of saying 'we do not want to discuss these issues now'.

Third, in particular, China singled out the issue of cross-border data flows, by stating that '[i]t's undeniable that trade-related aspects of data flows are of great importance to trade development'.[93] Interesting to note is, however, what China did and did not say in this sentence. It did not, for example, use 'free flow of data', which is how the United States has always referred to the issue in its submissions.[94] On the other hand, it qualified 'data flow' with 'trade-related aspects'. This implies that China is not willing to address all kinds of data flows, just those related to trade. In other words, to the extent that some data flows do not have a trade nexus, they could be legitimately excluded. As I have mentioned elsewhere, this qualification could have wide implications, as it could be employed to justify restrictions on data flows in sectors that China has not made commitments, or even for those covered by

[89] WTO, Joint Statement on Electronic Commerce, Ministerial Conference, 11th Session, Buenos Aires, 10–13 December 2017, WT/MIN(17)/ST/60 (2017).

[90] L. Kihara, 'DAVOS – Nearly Half WTO Members Agree to Talks on New E-Commerce Rules', *Reuters*, 25 January 2019.

[91] WTO, Joint Statement on Electronic Commerce, Communication from China, INF/ECOM/19, 24 April 2019.

[92] Ibid.

[93] Ibid.

[94] See WTO, Work Programme on Electronic Commerce, Non-Paper from the United States, JOB/GC/94 (2016), which refers to 'free flow of information' in para. 2.3, and INF/ECOM/5, which refers to 'free flows of information' in section 2.

existing commitments but provided free of charge (such as Google's search engine services), as they are not 'traded'.[95]

Fourth, in an effort to turn the table, China also prefaced the discussion on these 'other issues' with the recognition that members shall have the 'legitimate right to adopt regulatory measures in order to achieve reasonable public policy objectives'. This language is reminiscent of the calls for more 'policy space', a term often employed in trade negotiations to justify special and differential treatment and resorting to exceptions clauses. As the *China – Publications and Audiovisual* case mentioned earlier has illustrated, China will, most likely, invoke the public order exception contained in the general exceptions clauses of both the GATT and GATS to justify its online censorship regime. In particular, regarding data flows, China emphasized that it 'should be subject to the precondition of security' and should 'flow orderly in compliance with Members' respective laws and regulations'. This extends China's domestic narrative of cybersecurity to the international level, which is made complete with the earlier reference for all members to 'respect the Internet sovereignty' of other members. By elevating the issue to one of 'sovereignty', China has shown the seriousness it attaches to the issue of regulating data flow.

In summary, China has made it clear that it is not yet ready to discuss these sensitive data-related issues, at least not in the early stages of the negotiations. There is a possibility that it will consider some of them further down the road, but such negotiations will not be easy given China's guarded position.

D CONCLUSION

When people discuss data regulations today, they tend to focus on two main players: the UnitedStates, which calls for free flow of data to serve the interests of firms, and the EU, which prioritizes the need for the protection of personal information and privacy of the consumers. This chapter discusses the third major player – China – which emphasizes data security and even regards it as a matter of national sovereignty. Of course, such a regulatory approach was not formed overnight. Instead, the earlier discussions have illustrated how data regulation with Chinese characteristics has evolved over the past twenty-five years. More specifically, the analyses in this chapter have shown the differing regulatory logics and approaches at two different levels – the national and the international.

First, at the domestic level, we have seen Internet regulation shifting from hardware to software, and now to content and data. The shift in regulatory focus closely follows the development of the Internet in China, where it started as a novelty that was confined to the ranks of tech-savvy geeks, then gradually expanded to the masses with the proliferation of software and apps catered to popular uses, and now permeates everyone's daily life from socializing and shopping to entertainment

[95] Gao, note 86.

and education. Recognizing the central role played by the Internet in modern life, Chinese regulators have shrewdly chosen to regulate data, which is the essence of cyberspace that powers everything, especially with the rise of big data and artificial intelligence. Moreover, data regulation has now been elevated to the level of national security, and the agency that is responsible for content regulation, the CAC, has also evolved into the super-agency that is almost synonymous with data regulation in China. The CAC has no responsibility in promoting the growth of the sector. Instead, its only responsibility is making sure that the cyberspace is secure and nothing unexpected pops up. It is this single-minded pursuit of security that has led to such draconian policies as Internet blockage, filtering and other restrictions on the free flow of data, forced data localization requirements and the transfer of source code. As the Internet is becoming more complicated and omnipotent, we can only expect Internet and data regulations in China to become more sophisticated and omnipresent.

Second, at the international level, due to its unpleasant experience in WTO disputes, China has for a long time been rather cautious in addressing Internet and data related issues. This approach is also reflected in its free trade agreements, which tend to avoid the Internet-related issues. Even though its most recent FTAs – especially the ones with South Korea, Australia and Chile – started to address them, they tend to focus on only e-commerce-related issues and do not really address data flows. At the same time, in contrast to its defensive position on data-related issues, China has been quite aggressive in pushing for liberalization of 'cross-border trade in goods enabled by Internet'. This reflects China's interest as the leading goods exporter and the success of its e-commerce platforms such as Alibaba. In its latest proposal on the WTO Joint Statement Initiative on e-commerce, China started to address data regulations, but they were framed as secondary issues that require 'more exploratory discussions' and are subject to each member's 'right to regulate' to achieve other policy goals, especially security.

The growth of the Internet in China over the past twenty-five years has not only led to the phenomenal growth of its e-commerce market, but also gave China the confidence and power to export its model, and to 'set the agenda and make rules for cyberspace at the international stage', as per the high-level exhortation by President Xi at the Politburo's Thirty-Sixth Collective Study Session on 'Implementation of the Internet Power Strategy' in October 2016.[96] The success of China's e-commerce sector will make the Chinese model attractive to many developing countries, as many of them are trying to emulate the accomplishments of China. However, an argument could be made that given China's huge population base and the resulting

[96] Xi J., 'Accelerate the Promotion of Indigenous Innovation on Internet Information Technology, Strive Unrelentlyly towards the Objective of Building the Internet Power [Jiakuai Tuijin Wangluo Xinxi Jishu Zizhu Chuangxin, Chaozhe Jianshe Wangluo Qiangguo Mubiao Buxie Nuli]', *Xinhua News*, 9 October 2016.

enormous market, its e-commerce success story is more 'in spite of', rather than 'because of', the tight grip on cyberspace by the government. Nonetheless, given China's growing economic clout, data regulation with Chinese characteristics is something that the rest of the world must grapple with for some time to come. It is in this regard that this chapter tries to make a distinct contribution by offering a preliminary peek behind the cyber curtain, while also offering some hints on the things to come.