Centre for International
Governance Innovation

Conference Report – Virtual Workshop, November 28, 2022

Digital Governance in China
Data, AI and Emerging Technologies, and Digital Trade

Alex He and Robert Fay

Centre for International
Governance Innovation

Conference Report – Virtual Workshop, November 28, 2022

Digital Governance in China
Data, AI and Emerging Technologies, and Digital Trade

Alex He and Robert Fay

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Program Manager Jenny Thiel
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

Centre for International Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

vi About the Authors

vi Acronyms and Abbreviations

1 Introduction

1 Key Takeaways

3 Data Governance in China

7 Governance of AI and Emerging Technologies in China

10 China's Participation in Digital Trade

12 Conclusion

13 Agenda

15 Participants

About the Authors

Xingqiang (Alex) He is a CIGI senior fellow. He is an expert on digital governance in China, the Group of Twenty (G20), China and global economic governance, domestic politics in China and their role in China's foreign economic policy making, and Canada-China economic relations.

Prior to joining CIGI in 2014, Alex was a senior fellow and associate professor at the Institute of American Studies at the Chinese Academy of Social Sciences (CASS) and a visiting scholar at the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, in Washington, DC (2009–2010). Alex was also a guest research fellow at the Research Center for Development Strategies of Macau (2008–2009) and a visiting Ph.D. student at the Centre of American Studies at the University of Hong Kong (2004).

Alex is the author of *The Dragon's Footprints: China in the Global Economic Governance System under the G20 Framework*, published in English (CIGI Press, 2016) and Chinese editions, and co-author of *A History of China-U.S. Relations* (Chinese Social Sciences Press, 2009). Alex has published dozens of academic papers, book chapters, and newspaper and magazine articles.

Alex has a Ph.D. in international politics from the Graduate School of CASS and previously taught at Yuxi Normal University in Yunnan Province, China. Alex is fluent in Chinese and English.

Robert (Bob) Fay is a highly accomplished and respected leader in the field of digital economy research. With more than 30 years of experience working in the public and private sectors, he has developed expertise in economics, policy analysis and strategic planning.

Currently, Bob serves as managing director of digital economy at the Centre for International Governance Innovation (CIGI), where he leads a network of researchers focused on the intersection of technology, trade, innovation and governance. In this position, he has played a key role in shaping the discourse around the digital economy and has contributed to numerous policy debates and research initiatives on topics such as data governance, digital innovation and the future of work.

Before joining CIGI, Bob held various leadership positions at the Bank of Canada (BoC), where he was responsible for the assessment of digital technologies for Canada's economy and international economic developments, and provided short-term forecasting, structural analysis and policy advice. He was also special assistant to BoC Governor Mark Carney and his chief of staff, playing a key role in delivering policy direction. Bob began his career as an economist at the Organisation for Economic Co-operation and Development, where he worked on labour market issues and country-specific analyses.

Bob holds an M.A. in economics from Queen's University and has published numerous research papers and policy briefs on a range of economic and policy topics.

Acronyms and Abbreviations

AI	artificial intelligence
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
CIGI	Centre for International Governance Innovation
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEPA	Digital Economy Partnership Agreement
GDPR	General Data Protection Regulation
IP	intellectual property
IT	information technology
MIIT	Ministry of Industry and Information Technology
PIPL	Personal Information Protection Law
R&D	research and development
RCEP	Regional Comprehensive Economic Partnership
WTO	World Trade Organization

Introduction

China's massive presence in the digital economy is defined by its focus on big data, artificial intelligence (AI) and other emerging technologies, digital trade, standards, intellectual property (IP) and innovation. Further, digital governance in China constitutes a significant global issue at the intersection of technology and international governance. At the same time, the ongoing technological and trade decoupling between the United States and China may have dimmed the future of the digital economy and high-tech development in China. The long-awaited Chinese Communist Party's (CCP's) 20th National Congress in October 2022 concluded with a norm-breaking third term for President Xi Jinping as the party's general secretary, consolidating unprecedented power among Xi and his loyalists (not seen since Chairman Mao Zedong) in the top leadership positions, which has left more questions and uncertainties for the future of China.

In the context of these latest developments, the Centre for International Governance Innovation (CIGI) organized and hosted a virtual workshop on November 28, 2022, to examine the status and future development of China's digital governance practices. With experts from Canada, China, Europe, Singapore and the United States, the workshop discussed China's digital governance practices in three critical areas: data governance, governance of AI and other emerging technologies, and China's participation in digital trade to shed light on the country's digital governance and its international implications.

This conference report shares key takeaways from the workshop, which was held under the CIGI Rule.[1] The workshop summary does not purport to represent a consensus among the participants, nor to convey the views of any individual or organization. Rather, its goal is to review the latest developments in China's digital governance, in particular in the three areas mentioned above to demonstrate the global impact of the country's digital governance system.

1 See www.cigionline.org/about/cigi-rule/.

Key Takeaways

Data Governance

- The enormous economic value of data is a key to understanding China's data governance system, which is different from the data protection frameworks in Europe that primarily focus on protecting the individual's right to privacy, and practices in the United States that focus on regulating private law relationships between economic players and protecting individuals from government intervention.
- China's data protection framework has evolved to consist of two major pillars: the Personal Information Protection Law (PIPL) and the Data Security Law. The former is primarily concerned with data by which individuals can be identified but is not a legal framework that deals with any kind of data. The latter, with its vague definition of key terms and wide coverage of potentially all data, makes China unique among major digital players as it essentially protects national security, the public interest and the collective against harm that might arise out of the misuse of any kind of data.
- A significant effort has been made to create a protective wall in China regarding the export of data and its accessibility to safeguard the economic value of data as well as to address national security as "securitization" has become a leading economic objective under President Xi. The future of outbound data transfers from China is in a state of flux. Regulations are becoming increasingly clear when it comes to cross-border data transfer while the vague terminologies on data governance remain in place. Regulators still retain a lot of leeway and can mandate an outbound data transfer assessment and block data export whenever they deem it necessary.
- Data security is clearly regarded as a very important part of China's national security strategy, and the crackdowns on digital and data trade regulations in the name of national security will continue after the 20th National Congress — everything in China can be connected to national security.
- China is building its own version of a digital economy to integrate with the real economy or the industrial sector. China's digital giants

have refocused on industrial sectors, such as those that develop AI and information technology (IT), to bolster high-tech innovation using China's digital and data capacity.

- Most of China's big digital platforms are transactions-based platforms related to payments and are therefore not innovative, although they have a large number of users and access to massive amounts of personal data. These platforms are now facing strict data supervision for violating personal data regulation after a period of wild growth. In that context, China's data regulation framework requires large digital platforms to take more responsibility to protect data security and personal information while stressing the need for data-driven economic development to maximize the value of data.

- Digitalizing the real economy and unlocking the potential of data is a top priority for China. In this sense, use of the term "crackdown" on the digital economy is misleading. Nevertheless, China's data governance regime is developing a dual-track trajectory. Data abuses by tech giants are severely punished while state entities have mostly free rein to collect citizens' information.

- Although the Chinese, EU and US regimes have very different starting points and different emphasis and values in specific areas of data privacy versus data as a national security issue versus rent capture in industrial policy, there appears to be some general convergence moving toward a framework with features from each. The antitrust actions that are being taken by China, Europe and the United States, as well as the fact that they all heavily engaged in industrial policy to capture rents, are two important technological conditions that are driving the convergence.

- Although there will be many obstacles en route to building a rules-based order for the digital economy, perhaps this can be achieved by negotiations rather than through unilateral actions such as harsh bans on the export of data, whether in China or the United States.

- China is pursuing multiple goals simultaneously and is seeking to balance trade-offs between the use of data as an economic resource and its role in domestic governance. This approach stands in contrast to the popular Western commentary framing data issues in China in binary terms: either totalitarian surveillance or personal information protection, either data localization or a competitive digital economy.

- The CCP is preoccupied with mass collection of Chinese citizens' data as a conduit to security and stability. However, big problems such as data silos continue to hinder the achievement of this data-driven governance.

Governance of AI and Emerging Technologies

- China has moved first in algorithm regulation relative to other major jurisdictions, especially in areas such as online delivery services and social media platforms. The Internet Information Service Algorithmic Recommendation Management Provisions, effective March 1, 2022, regulate the recommendation algorithms, setting an example for the West on how to regulate algorithms and tech companies. However, the key question for the far-reaching policy and incredibly ambitious regulations is whether they can be implemented.

- China's new regulation on recommendation algorithms has increased state control over the dissemination of information via vague definitions and rules forbidding algorithms from engaging in activities that harm national security or the public interest. At the same time, the regulation has also tried to protect worker and consumer rights, which gives Chinese internet users more consumer rights related to algorithms than users anywhere else on the planet.

- The policy dilemma for China developing emerging technologies is that leading technologies have been financed by venture capital, which is profitability driven and growth-stage investment oriented, and not well suited under the current geopolitically uncertain global environment.

- China's biggest problem in financing emerging technologies is its lack of patience. There is a lot of investment in emerging technologies because of foreign import substitution, but it is unclear whether this investment is sustainable.

- China has become the largest global source of top AI research talent, followed by the United States, the European Union and India. China led

all countries in the number of AI-related papers it published in 2020. Although China is trying to produce a lot of AI research and development (R&D), US companies and universities remain the driving force behind most of the game-changing breakthroughs, especially in recent years.

- With the US export control on high-end chips, including AI chips to China, there is not much China can do in the short term, but it will be very difficult for American tech companies to give up the huge market in China.

- Chinese regulators behave like start-ups: they fail fast and early. Under China's one-party system, implementing and updating policy does not involve arguing with many other parties. It is expected that regulators will see what works and what does not, and then release a series of policy updates and supporting regulations that define some of these more ambitious and vague rules.

- It is very clear that China's AI governance regulations and practices borrowed many ideas from the European Union, especially the risk-based AI classification system. China can contribute to global AI governance based on its rich AI applications and the challenges it faced.

Digital Trade

- China is very serious about joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA) and willing to meet their obligations as part of its promotion of high-level opening up. It would not be difficult for China to meet the requirements of the CPTPP and the DEPA as the exceptions within those agreements would allow China to do what it wants. With more than 600 pages of legally binding rules in the CPTPP, it is better to have China in the agreement than not, if China can meet the requirements to join. Still, it could be politically difficult for some members to agree with China's entry into the CPTPP and the DEPA, and it may be a much tougher task for China to join the DEPA than to join the CPTPP as the DEPA is a very young agreement (it entered into force in 2021), and there is significant risk if China joined on the ground floor since the DEPA is more a venue for shared values and norms, which are different in China. There are also political considerations that will play an important role.

- With either a weak or not very effective agreement or no regional agreement, the world would go back to a reinforcement of three different data or digital realms — of the United States, the European Union and China, with everyone else in between. This is not really a solution.

Data Governance in China

China's Data Governance Framework

Data has become a critical part of economic, social and governance policy making in China in recent years. In the development of China's data governance system, data was first defined as a factor of production, a source of value or productivity on par with land, labour, natural resources and so forth, which gives data an enormous economic value. This is a key to understanding China's data governance system as it is obviously different from the data protection framework in Europe, which is mainly focused on protecting individuals' privacy. It is also different from data governance practices in the United States, which focus on regulating private law relationships between economic players as well as protecting individuals from certain forms of government intervention.

Today, China's data protection framework has evolved into a comprehensive two-pillar system.

The first one is the PIPL, which builds on a longer trajectory of data-related regulations that emerged in the early 2010s and has now matured into a full-fledged legislative framework. The PIPL bears a clear family resemblance to Europe's General Data Protection Regulation (GDPR) in the objectives that it tries to achieve and the legal tools by which it tries to achieve them. In short, the PIPL is aimed at preventing harm to individuals arising from the abuse of personal information such as through telecom fraud and data theft. It is primarily concerned with data by which individuals can be identified, but it is not a legal framework that deals with any kind of data and does not regulate all possible uses of information.

The PIPL covered stipulations related to business models (for instance, how do large private companies use data in a way that might impact the economic rights and interests of users, the competition with and between platforms themselves, and third-party merchants operating on those platforms). It also contains fairly strict provisions on personal information exports, which demonstrates a growing concern in China about how information on Chinese citizens is being exported.

The second pillar is the Data Security Law, which makes China unique among major digital players as it essentially protects national security, the public interest and the collective against harm that might arise out of the misuse of any kind of data. It covers potentially all data, and it seeks to prevent public harm rather than private individualized harm. To that extent, it divides data into three categories: ordinary data; important data; and core national data with increasing security requirements, reporting and auditing standards, and limitations on the collection, processing, and trade and export of that data.

The problem with both laws is that much of the implementing regulations have yet to be made, especially the Data Security Law, which remains very vague, with broad mandates of charging ministries and compiling catalogues of data to be categorized under the three categories mentioned above. There are obviously technical difficulties associated with this process and also political steps to be made, as any form of regulation will create massive winners and losers. Progress has been achieved in some priority areas, such as the broad pharmaceutical regime, as well as the development of smart vehicles, including self-driving vehicles.

China's digital and data governance framework has two outstanding features that persist following the CCP's 20th National Congress.

First, data security is clearly regarded as a very important part of China's national security strategy, and this trend will definitely continue after the party's 20th National Congress. The national security crackdowns on digital and data regulations will continue because China overly focuses on national security. In addition, China's internet regulator, the Cyberspace Administration of China (CAC) that oversees data and digital regulation, does not have any corresponding responsibility for the development of the sector, which is the jurisdiction of the Ministry of Industry and Information Technology (MIIT) and the Ministry of Commerce. Data was mentioned only once in the 20th National Congress report and it was mentioned as part of the section on China's security strategy, where the report emphasized the need for strengthening the construction of security systems for the economy, major infrastructure, finance, networks, data, biology, resources, nuclear energy, space and the ocean.

Second, China is building its own version of a digital economy to integrate with the real economy or the industrial sector. This type of digital economy is different from that of the United States, which is home to digital giants such as Google, Facebook, Twitter and so on. Under President Xi's direction to build China into an industrial power, China's digital giants such as Alibaba and Tencent refocused from online payment services such as food and grocery delivery and online games and tried to move into industrial sectors, such as AI and IT, to bolster high-tech innovation using China's digital and data capacity. Although this is a clear focus, whether anything will materialize from it is another question.

Digital Platform Governance

Most of China's big digital platforms are based on transactions, not innovation. They include e-commerce platforms such as Taobao (owned by Alibaba), JD.com and Pinduoduo; online services platforms such as Meituan and ele.me; social media platforms such as WeChat and Xiaohongshu; and digital content platforms such as ByteDance, Bilibili and so forth. Benefiting from China's demographic dividends, these platforms grow very fast and have a large number of users and massive amounts of personal data.

With the PIPL and Data Security Law coming into effect and the introduction of implementation rules, including the Measures for Security Assessment of Outbound Data Transfer and Measures for Cybersecurity Review, an era of tough data regulation has begun after a period of rapid growth of these platforms. The drafted amendment for the Cybersecurity Law released in 2022 increased fines for violations of cybersecurity obligations.

As for digital platform governance, the balance between security and development and between domestic and international dimensions are worth noting.

These platforms have faced the risk of severe punishment for violating data-related regulation since last year. The CAC strengthened enforcement efforts in areas such as cybersecurity data, security and personal information protection, and increased exposure of typical cases such as the massive RMB 8 billion fine imposed on ride-hailing giant DiDi for data violation. On the one hand, platforms are taking more responsibility to protect data security and personal information as the legal framework becomes more robust. On the other hand, China has stressed the need for data-driven economic development. Both the Data Security Law and the PIPL promote data utilization while regulating data-processing activities. The laws put aside some contentious issues such as data ownership and focus on rights and obligations related to data processing and data utilization to maximize the value of data. In this sense, China's approach is far from what is being called a regulatory crackdown.

Most of the Chinese digital platforms are doing business in domestic markets, with only a few overseas users. For example, the vast majority of WeChat users are in China. ByteDance has many overseas users but has separate entities operating independently at home (Douyin) and abroad (TikTok). The differences in entities and where they operate may be one explanation for why and how China tends to be more conservative toward cross-border data flows; the recent international competition and confrontation in digital is another.

Cross-Border Data Flow Regulations

A significant effort has been made to build a protective wall in China to shield the economic value of data through its export and accessibility as well as to address national security as "securitization" has become a leading economic objective under President Xi.

At the same time, the data-driven economy has matured rapidly in China. And contrary to what some may believe, it has experienced an enormous expansion of cross-border data transfers since it is integrated into global manufacturing, probably more so than any other economy. Further, with the Digital Silk Road initiative, China also has had a chance to capture global economic rents in the data space. Its moves to accept data commitments on the free flow of data and no data localization in the Regional Comprehensive Economic Partnership (RCEP) and its application to join the CPTPP make sense in that context.

The future of outbound data transfers from China is obviously in a state of flux. On the one hand, the Chinese government has no intention to ban everything or to localize all data and stop outbound flows of data across the board, and its PIPL includes a clause indicating China's willingness to negotiate cross-border data transfer agreements with other jurisdictions. There are mechanisms such as standard contractual clauses or a certification mechanism for the transfer of personal data in its latest draft regulation from summer 2022. The CAC has released the cross-border rule for data transfer, which clarified the process through which the CAC reviews outbound data transfer requirements. This means that regulations are becoming increasingly clear when it comes to cross-border data transfers. Obviously, regulators still retain a lot of leeway. The CAC still mandates an outbound data transfer assessment and blocks data export whenever it is deemed necessary.

On the other hand, the vague terminologies on data governance still exist. There is a need to clarify further what constitutes important data and what constitutes core national data, which obviously raises questions for other jurisdictions and companies as well. There are concerns about inbound data transfers to China. The debate in the European Union and the United States on how to regulate TikTok reflects the concern of how much the Chinese state is codifying and accessing privately held data sets that contain personal data. This complicates inbound data transfers to China to the extent that other jurisdictions may not trust China's government in keeping data secure.

To some extent, the world digital market is being divided into two separate markets: the global market without China and the Chinese market, which stands in contrast to the global nature of the digital economy. At the same time, as digital globalization is moving forward, traditional economic globalization is standing still or even going in reverse. Only by integrating into the global market can China seize the opportunities of digital globalization.

Building a rules-based order for the digital economy comes with many complications, but perhaps negotiations can be used to achieve this goal rather than unilateral actions such as harsh bans on the export of data in China or the United States.

Policy Trade-Offs in China's Data Governance Practices

Much like other jurisdictions, China's government is balancing different policy objectives in data governance between data as an economic resource and security concerns over the uses of data. This is important to highlight as it contrasts with the popular Western perspective that views data issues in China as an either/or scenario: either totalitarian surveillance or personal information protection, either data localization or a competitive digital economy.

Regulators in China are pursuing multiple goals at the same time and trying to balance these different trade-offs, which are quite difficult to achieve for China or any other jurisdictions. The Chinese government has no intention of protecting everything or excluding all types of data from domestic and cross-border exchange and trading, which is where the data classification process under the data security law comes in. Digitalizing the real economy and unlocking the potential of data is a top priority in China. In this case, the term "crackdown" on the digital economy is misleading. Collecting, analyzing, processing and sharing data effectively and productively is a precondition to achieving that objective. In Chinese policy terms, this is called "informatization," meaning to digitalize everything, which entails several approaches with respect to data.

First, there is a policy trade-off in the creation of a state-led national data market. The Chinese government is trying to create a functioning market where companies can buy and sell their data sets and make a profit. The problem is that companies do not have the incentives to participate in data markets, put their data sets to use and share them openly via data exchange platforms. The central government is now starting to work on a new batch of data exchanges to try to persuade market actors to use them. The trade-off here is between state control and marketization: To what extent is Beijing willing to push for these state-led marketplaces to become the default for data trading in China? Considering that one objective is to fight monopolies, to increase economic productivity and public welfare, tension between the state and market actors may continue to be part of this process.

Second, a policy trade-off exists between the CCP's obsession with mass data collection of its citizens to maintain security and stability and the high standards of data protection and data security the party wishes to achieve. Chinese leaders believe data-driven governance is the key to social stability and regime security. The CCP aspires to have data-driven, AI-enabled predictive products to keep tabs on any perceived threats to its rule, for example, protests. However, data silos that have hindered the achievement of data-driven governance are a big problem. For example, the government has tried for years to close data silos in the public security sector to better merge different pools of data such as surveillance data or police data (for instance, facial recognition footage from surveillance cameras). The work is still in progress, and officials continue to complain about the issues with data silos.

More generally, China's data governance regime is developing along a dual-track trajectory. On the one hand, data abuses by tech giants are severely punished. On the other hand, state organizations have mostly unfettered access to collect and harvest citizens' information, even against their consent, as the state's security-motivated exemptions are written into all key laws, including in the PIPL.

Third, there is a policy trade-off between digital transformation and environmental protection. Data governance in China is not only accomplished through laws and regulations but also through industrial policy. Processing and storing data requires a huge amount of energy. China, like other countries, faces this major environmental challenge in advancing its digital transformation. In 2020, China's data centre power consumption was projected to grow by 65 percent until 2023, which is equal to the carbon emissions of a mid-sized country. The campaign to roll out digital infrastructure or new fifth-generation networks, data centres, cloud computing, AI facilities and so forth can be at odds with China's lofty ambitions for its green transition. China is working to improve the layout of national data centres, trying to transfer data from coastal areas of China to more resource-rich provinces in the west to improve energy efficiency. And the MIIT has also further raised its requirements for data centre power usage efficiency to try to solve that problem.

Convergence of Regimes for Data Governance in the European Union, United States and China

Technology should be driving convergence toward a structure that is efficient for the economy. To the extent that new technologies open up a major new source of economic rent, the rivalry to capture those rents inevitably leads to frictions. This applies to digital transformation and data governance.

It was not necessary to have one uniform regime for data governance in the pre-digital era. This was the starting point for regimes in Europe, the United States and China. In the absence of national champions, which are able to commercially exploit data, the European Union's natural incentives were to regulate data abuse, protection of personal privacy and antitrust measures. The European Union has since moved toward a system that emphasizes data, sovereignty and strategic autonomy, and then moved to engage in industrial policy with its digital single market exercise. It is now developing its own internal market to capture some of these rents. The United States has national champions and the data-driven economy, so the scope for data for global rent capture for the United States naturally led to concepts such as the free flow of data and no data localization and light-touch regulation domestically. These incentives reflect the starting points for the United States. They are not necessarily the endpoint for a mature system of data regulation.

China's trajectory has more or less followed a similar path as the United States, where it started with no general regime but has now moved toward an EU GDPR style. Although these regimes have very different starting points and different emphasis on specific areas such as data privacy versus national security of data versus rent capture in industrial policy, what can be seen is the general convergence of all three regimes toward a structure that features all three areas. The antitrust actions that are being taken by Europe, the United States and China, as well as the fact that they all heavily engaged in industrial policy to capture rents, are two important technological conditions that are driving the convergence. In the short run, as the digital economy matures and competition erodes the rents, there will be no economic peace or a rules-based order. But in the long run, governments move in the direction of the most efficient path. There are practical ways to deal with these three major areas, and governments are discovering their way forward. China will likely be moving in ways that ultimately will be compatible with other major jurisdictions.

Governance of AI and Emerging Technologies in China

AI Governance in China: Status and Future Direction

In recent years, China issued three data governance laws that include measures related to AI governance, as well as regulations to strengthen the ethical governance of science and technology while promoting the development of the AI industry as part of the global wave of AI governance.

To better regulate AI and algorithms, the China Academy of Information and Communication Technology under the MIIT issued a comprehensive framework on AI governance that includes the idea of trustworthy AI and built test platforms to demonstrate what trustworthy AI means. At the industrial level, some big enterprises such as Alibaba and SenseTime have established technology ethics committees consisting of reputational scientists, economists and researchers from public administration to foster better AI governance and create an inner synchronized assessment pipeline to avoid the potential risks of AI applications and the delivery of products and services.

It is very clear that AI governance regulations and practices in China have borrowed extensively from the European Union, especially the risk-based AI classification system. This similarity can also be seen in China's Data Security Law and the PIPL. In local-level regulations in Shenzhen, more discretion is given for experiments on what are known as low-risk scenarios. For example, if something goes wrong with a test product or service provided by an AI start-up, and it poses no threat to national security, the public interest or citizens' personal safety, no punishment would be applied. The risk-based AI classification system is important because AI technology is generally defined and can be applied widely. Even at the central level,

the government has also mentioned that AI regulations should create classifications to deal with different scenarios and different levels of risk.

In the future, China will focus on building an AI governance mechanism following these steps:

- First, form a value consensus that consists of the principles of inclusiveness, sharing, prudence and responsibility.
- Second, complete the division of value in AI governance, or build interactive and collaborative mechanisms between regulators and governance subjects, such as AI technology users and providers.
- Third, keep the interactive and collaborative AI governance mechanism agile, adaptive and exploratory as required by the rapidly evolving AI technology and changing preferences and governance demands of AI governance subjects.

China can contribute to global AI governance using its rich experiences with AI applications in a variety of fields. China's experiences, including the challenges it faced, could benefit other parts of the world in terms of developing AI governance, as shown in the "Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)" that China issued in November 2022, which is based on its AI governance practices and related challenges.

China's Emerging Algorithm Governance Rules

Chinese regulators have done a lot of work on AI ethics to create foundational ideas about ethical AI principles. Algorithm regulation has become a hot topic in China in recent years, especially in areas such as online delivery services and social media platforms. The Internet Information Service Algorithmic Recommendation Management Provisions that came into effect in March 2022 had broad implications for the internet in China.

This policy is designed to regulate a specific use case of algorithms known as recommendation algorithms. A recommendation algorithm looks at content that a user has viewed in the past and then recommends an advertisement based on that content or data, or it looks at what is in a user's shopping cart and what they purchased in the past and then offers product recommendations based on that data. This regulation takes a slightly broader view of what a recommendation algorithm is and looks at things such as maximizing the efficiency of delivery driver schedules.

On the one hand, the policy increased state control over the dissemination of information and the way that algorithms work, and one of the ways that state control is increased is through vague definitions that are included in the policy. Article 6 of this rule essentially states that any recommendation algorithm must uphold mainstream values or positive energy, but there is no legal definition of what "positive energy" is or what "mainstream values" are. This lack of clarity leaves those rules up to state interpretation and gives regulators a lot of discretion over what kind of information recommendation algorithms are allowed to disseminate, and what kind can be cracked down upon.

The policy also forbids algorithms from engaging in activities that harm national security or the public interest. The fact that "national security" and the "public interest" are not defined means that anything could potentially fall into the policy's scope. The policy also states that any algorithms that have "public opinion attributes or social mobilization capabilities" must register with the CAC, China's internet regulator, and must submit to a security risk assessment by the CAC, and algorithm providers are responsible for ensuring machines do not spread illegal and politically sensitive information. By doing so, the state is essentially requiring big tech companies that run these algorithms to decide what kind of content the public is going to consume, and what kind of products the public is going to buy. The CAC even required tech companies to submit basic information about their algorithms and created a searchable public database of the algorithms to make it convenient for regulators looking at how those algorithms could be regulated.

On the other hand, the rules have also tried hard to protect worker and consumer rights. Under this policy, Chinese internet users now have more rights related to algorithms than users anywhere else in the world. These rules essentially go much further than the European Union at this time in terms of protecting the rights of internet users who are being targeted by recommendation algorithms.

Under the policy, Chinese internet companies are required to inform users when they are being targeted with algorithm-driven recommendations

and let them opt out and choose to see only generic content that does not take their personal data into account. The policy also forbids algorithms from tagging users with illegal or discriminatory keywords. For example, users cannot be tagged based on their ethnicity or religion. The policy also requires internet companies to show users which keywords are being used to target them and delete those keywords. It also seeks to clamp down on misinformation around prohibiting algorithmically generated news. This rule can prevent internet companies from using a program or an algorithm that goes into a user's search history, looks at keywords and then cobbles together news content designed to manipulate the user's thinking. The policy also forbids algorithms from faking likes, comments, forwards or real human engagement, and prohibits the use of algorithms that violate labour rights, spread harmful content to minors, scam people (especially the elderly) and impose differential trade conditions (such as prices).

Contrary to the view that there is nothing to learn from China's tech policy, this particular regulation can set an example for the West on how to regulate algorithms and tech companies. The biggest concern is what happens if this regulation restricts tech company income and the development of the tech sector and digital economy.

The key question for the far-reaching policy and incredibly ambitious regulations is whether they can be implemented. Some of these rules can be enforced easily and others cannot. An interesting observation is that Chinese regulators behave like start-ups, failing fast and early. Under China's one-party system, the government does not have to argue with too many other parties in order to implement and update policy. Regulators will see what works and what does not, and then release a series of policy updates and supporting regulations that define some of the more ambitious and vague rules that have come out of a particular regulation.

Nevertheless, China can be an example of what to watch for regarding the implications of these regulations as algorithms are regulated more heavily. There will likely be lessons that other jurisdictions can draw on in their own regulation.

Developing Emerging Technologies in China under US Export Restrictions: The Venture Capital Perspective

The dilemma for China is its long-term goal of playing technological catch-up with the United States by focusing on tech applications and global sourcing, which is no longer sustainable given the stricter US export restrictions at a time of plateauing free trade. A lot of industries, global products and services may not be available to China anymore, therefore the country is basically entering a period of forced import substitution. The policy dilemma for China in developing emerging technologies is that leading technologies have been financed by venture capital, which is profitability driven and growth-stage investment oriented and not well suited to the current geopolitically uncertain global environment.

China now needs to support high-risk, early-stage small and medium-sized tech enterprises and transition to longer-term state venture funding. The Chinese government has supported initiatives that are not necessarily profitable, whereas the private sector is focused mainly on profitability. At this stage, the government and private sector have to collaborate whether they like it or not.

In response to stricter chip restrictions from the United States, a lot of private venture capital funds and government guidance funds have flowed into China's semiconductor industry. This trend picked up in 2021 following the ban on Huawei.

But China's biggest problem is that it needs more patient capital in financing emerging technologies. There is a lot of money in emerging technology because of foreign import substitution. But it is not yet clear whether the investment is sustainable. On average, venture capital funds usually have a 10-year life cycle plus a two-year possible extension. But in China, the life cycle is typically three years plus five years, sometimes even less. Perhaps China can learn from its industries in solar photovoltaics and electric cars, where government support was gradually withdrawn.

Western Countries' Cooperation with China on AI R&D

Although China is trying to produce a lot of AI R&D, US companies and universities remain the driving force behind most of the game-

changing breakthroughs, especially in recent years. There exists cooperation between China and the United States and its allies such as the European Union and Canada on AI R&D, and this collaboration can be identified by five indicators.

First, international students account for very significant majorities across all graduate-level science and engineering programs at US universities. Chinese students' enrollment in graduate-level computer science programs at US universities was second only to Indian students in 2017 and 2018. Chinese engineering graduate students outnumbered Chinese computer science students, and at the Ph.D. level, China leads in the cumulative number of US doctorate recipients over the last 20 years or so.

China has become the largest global source of top AI research talent, followed by the United States, the European Union and India, which certainly had an enduring impact on AI R&D outside of China. Most of these Chinese students choose to attend graduate school in the United States. The vast majority (about 89 percent) of Chinese researchers who attend US graduate schools stay to work in the United States and publish cutting-edge research. This pipeline of research talent is expected to decline due to the negative impact of COVID-19 and the chilling effects caused by a policy during Donald Trump's presidency to restrict access of Chinese students with any involvement in China's military civil fusion strategy.

Second, China led all countries in the number of AI papers published in 2020, but only 12 percent of them are co-authored AI publications, which usually received significantly higher citation counts. From the US perspective, Chinese researchers are the top collaborators on AI papers, followed by those from the European Union, Canada, Australia, Japan and Singapore.

The third indicator is the publication of AI research and the fourth is the number of AI conferences hosted by country, which is an important pathway for dissemination of information. The United States leads by a wide margin, with half of the 16 recent and future major AI conferences scheduled in that country, followed by Canada and China.

The fifth factor is the number of US private labs overseas. American big tech companies such as Amazon, Apple, Facebook, Google, IBM and Microsoft have about 70 percent of their AI labs outside the United States. Most are in Europe, mainly the United Kingdom and France; there are also labs in Israel and China. About 10 percent are in China. Chinese AI company Baidu has a significant lab outpost in Silicon Valley in the United States. But with the growing ethical, competitive and geopolitical concerns about China, these types of interconnections have come under increasing scrutiny.

With China facing the US export control on high-end chips, including AI chips, there is not much it can do in the short term, but it is very difficult for American tech companies to give up the huge market in China. To date, Chinese nationals studying and working in the United States have not been caught up in this rule, and collaboration on AI R&D with non-US nationals will continue.

China's Participation in Digital Trade

China and the Governance of International Digital Trade

A trade agreement can help focus attention, limit the actions that governments may take, provide more certainty and lower risks. It can also create more opportunities for companies that demonstrate profitability, competitive advantage, market leadership, good management and so forth. But the challenge facing any trade agreement is that it does not constrain big players who do not want to follow the rules of the trade agreement, as can clearly be seen in the World Trade Organization (WTO) system. But small players break the rules as well. The challenge always is how to hold them accountable and how often to hold them accountable.

There are no global rules for digital trade. There are some regional rules in data and digital agreements, but they have many loopholes and exceptions. The global rules are unlikely to be easily reached in the digital space because even the governments that are enthusiastic about signing agreements are unclear about what those rules should look like, and how they should be implemented.

China's position on digital trade agreements is that there should be no duties on e-commerce, and it supports the WTO's moratorium on imposing duties, tariffs and taxes on electronic transactions. This position can be seen in the WTO Moratorium on Customs Duties on Electronic Transmissions and also in the RCEP and in China's free trade agreements with Australia, New Zealand and others.

The likelihood of whether an international agreement on digital trade is reached or not depends on if there is enough common ground among the three data realms: China, the European Union and the United States. But even if there is an agreement, it will be very weak, like the version of the data draft for trade-related aspects of e-commerce at the WTO. It is probably along the lines of the e-commerce chapter in the RCEP, in which a country such as China would be able to use national security to ultimately impose legitimate restrictions on cross-border data flows that cannot be disputed. An agreement like this would not foster or support digital trade and cross-border data flows.

With a weak or not very effective agreement or no regional agreement at all, the world would go back to the reinforcement of three different data or digital realms, which is not really a solution. The United States makes it more difficult by creating the Global Cross-Border Privacy Rules Forum as part of its Indo-Pacific Economic Framework, trying to pull the cross-border privacy rules out of the Asia-Pacific Economic Cooperation forum. This would make it more incompatible with the European Union's GDPR and creates more challenges for countries in between, such as Australia, Canada or Japan.

For China, there is substantial unrealized potential with respect to the digital economy as some capacity constraints are still impeding its engagement in this sector. The constraints also apply at the border and to China's embrace of digital trade agreements. The Organisation for Economic Co-operation and Development has developed an indicator for digital services trade restrictiveness, which considers discrimination against foreign supply and market access with respect to infrastructure, connectivity, electronic transactions, payments, IP rights in the digital realm and other barriers to digitally enabled services, such as access to cross-border digital trade, downloading and streaming. China's trade restrictiveness score as of 2021 indicates that it is four times more restrictive than a typical advanced economy.

This constraint will have a negative impact on innovation. The indicator of private R&D expenditures is important since R&D is an input for innovation processes. The annual data on R&D expenditures among the top 2,500 firms since 2014 shows a highly significant and negative relationship between digital trade services and trade restrictiveness. If the source of most technologies around the world is imported, barriers to market access would affect innovation, and impediments to digital inputs would limit China's capacity for its own technological development.

China's Prospects for Joining the CPTPP and the DEPA

China is very serious about joining the CPTPP and the DEPA as part of its promotion of high-level opening up, and it is willing to meet the obligations when it comes to the digital trade sector. From China's perspective, the top leadership would try to relax data regulations such as restrictions on cross-border data flows to meet the rules and requirements for joining the CPTPP and the DEPA to promote economic development and China's model overseas. The gap between the new obligations in both the digital trade chapter in the CPTPP and the DEPA, and China's existing obligations in the RCEP, is not that wide. That is not the most challenging issue.

The main reason why it would not be that difficult for China to meet the requirements to join the CPTPP and the DEPA is the exceptions within those agreements that would allow China to do practically whatever it wants. The CPTPP's rule on data flows and data localization has many exceptions that are broad and unclear, which makes it hard to hold any country accountable. For example, the fact that it is not clear what a legitimate public policy objective means as an exception to applying restrictions on data could enable China to claim that restricting data flows and requiring permission for data to leave China is in the pursuit of a legitimate public policy objective. Further, the language in the RCEP's digital trade and e-commerce chapters is built on the CPTPP, but it dilutes or weakens the language in the CPTPP. China's push for that kind of language in the RCEP is a strong indication that the country ultimately wants to be allowed to impose whatever exceptions it wants on cross-border data flows.

At the same time, there is no alternative to these rules in trade agreements such as the CPTPP and the DEPA. With more than 600 pages of legally binding rules in the CPTPP, it is better to have China in the agreement than not if it can meet the rules and requirements.

The DEPA is slightly different and more challenging for China to join than the CPTPP as the DEPA is not just about the rules and how to follow them but much more about how to create rules for the future. It is more about shared values and norms, which would be at risk if China joined on the ground floor because of the country's different values. One of China's motives for joining the DEPA is to try to get into organizations through multilateral trade frameworks and shape these frameworks. However, China could still join the DEPA as the agreement has some exceptions from the commitments that are particularly important.

Whether China can join the CPTPP and the DEPA also depends on how other member countries such as Canada and New Zealand see the issue. It could be politically challenging for some members to agree on China joining. For example, it would be difficult for Canada to accept China into the CPTPP in the current political context. Furthermore, China's lack of diplomacy in seeking to join the DEPA was not helpful: the country announced that it would join the DEPA when none of the three founding members of the agreement were present.

Conclusion

Three distinct features stand out in China's digital governance. First, digitalizing the real economy and unlocking the potential of data is a top priority in China. Second, China has moved first in some key areas of digital governance such as digital platform and algorithm regulations, but whether these regulations can be implemented remains uncertain. Third, data security is clearly regarded as a very important part of China's national security strategy.

However, it is fair to say that China, like other countries and regions, is struggling to find that balance between cybersecurity, privacy, economic development and innovation in terms of digital governance. Technology should be driving convergence toward a structure that is efficient for the economy. In the long run, there is a general convergence moving toward a structure that features data privacy, data security and data's economic value in China, Europe and the United States. But in the short term, there will be many frictions along the path to building a rules-based order for the digital economy.

The participants of the workshop agree that there is a lot of work left to do in research on digital governance in China and its implications for the world, and discussion on these issues should continue to explore constructive and compatible ways to build a rules-based global digital economy.

Agenda

November 28, 2022

9:00–9:10 **Introduction**

- → **Bob Fay**, Managing Director of Digital Economy, CIGI

Opening Remarks

- → **Paul Samson**, President, CIGI

9:10–10:10 **First Panel: Data Governance in China: Platforms, Competition, Standards**

- → **Moderator: Henry Gao**, Law Professor, Singapore Management University; Senior Fellow, CIGI
- → **Rogier Creemers**, Co-founder, DigiChina; Assistant Professor, Leiden University
- → **Mosi Li**, Professor, Shanghai University of International Business and Economics
- → **Rebecca Arcesati**, Analyst, Mercator Institute for China Studies (MERICS)
- → **Dan Ciuriak**, Director and Principal, Ciuriak Consulting; Senior Fellow, CIGI

Round Table Discussion and Q&A

10:10–10:15 **Health Break**

10:15–11:15 **Second Panel: Governance of AI and Emerging Technologies in China**

- → **Moderator: Rohinton P. Medhora**, Distinguished Fellow, CIGI
- → **Zheng Liang**, Professor, School of Public Policy and Management, and Vice President, Institute for AI International Governance, Tsinghua University
- → **Kendra Schaefer**, Head of Tech Policy Research and Partner, Trivium China
- → **Anton Malkin**, Assistant Professor, Chinese University of Hong Kong, Shenzhen; Fellow, CIGI
- → **Joshua P. Meltzer**, Senior Fellow, Global Economy and Development, Brookings

Round Table Discussion and Q&A

11:15–11:20 **Health Break**

11:20–12:20 **Third Panel: China's Participation in Digital Trade: Data Flows, Privacy, IP**

- → **Moderator: Susan Ariel Aaronson**, Research Professor, Elliott School of International Affairs, The George Washington University; Director, Digital Trade and Data Governance Hub; Senior Fellow, CIGI
- → **Henry Gao**, Law Professor, Singapore Management University; Senior Fellow, CIGI
- → **Patrick Leblond**, Associate Professor, University of Ottawa; Senior Fellow, CIGI
- → **Deborah Elms**, Founder and Executive Director, Asian Trade Centre; President, Asia Business Trade Association
- → **Douglas Lippoldt**, Senior Fellow, CIGI

Round Table Discussion and Q&A

12:20 **Closing Remarks**

- → **Bob Fay**, CIGI

Participants

Susan Ariel Aaronson
Research Professor, Elliott School of International Affairs, The George Washington University; Director, Digital Trade and Data Governance Hub; Senior Fellow, CIGI

Aya Adachi
Analyst, Mercator Institute for China Studies (MERICS)

Daniel Araya
Senior Partner, World Legal Summit; Senior Fellow, CIGI

Rebecca Arcesati
Analyst, MERICS

Veronika Blablová
Data Analyst, Association for International Affairs

Vincent Brussee
Analyst, MERICS

Greg Cederwall
Senior Trade Policy Officer, Global Affairs Canada

Eugene Cheah
Graduate Student, Peking University's School of International Relations

Shenjie Chen
Director of Economic Research, Government of Canada

Dan Ciuriak
Director and Principal, Ciuriak Consulting; Senior Fellow, CIGI

Rogier Creemers
Co-founder, DigiChina; Assistant Professor, Leiden University

Deborah Elms
Founder and Executive Director, Asian Trade Centre; President, Asia Business Trade Association

Paul Evans
Professor, School of Public Policy and Global Affairs, University of British Columbia

Bob Fay
Managing Director of Digital Economy, CIGI

Sridhar Ganapathy
Senior Associate, Artha Global

Henry Gao
Law Professor, Singapore Management University; Senior Fellow, CIGI

Tommaso Giardini
Associate Director, Digital Policy Alert

Michel Girard
Senior Fellow, CIGI

Anita Gurumurthy
Executive Director, IT for Change

Alex He
Senior Fellow, CIGI

Gurumurthy Kasinathan
Director and Lead, Education and Technology, IT for Change

Mark Kruger
Opinion Editor, Yicai Global; Senior Fellow, CIGI

Patrick Leblond
Associate Professor, University of Ottawa; Senior Fellow, CIGI

Mosi Li
Professor, Shanghai University of International Business and Economics

Zheng Liang
Professor, School of Public Policy and Management, and Vice President, Institute for AI International Governance, Tsinghua University

Douglas Lippoldt
Senior Fellow, CIGI

Anton Malkin
Assistant Professor, Chinese University of Hong Kong, Shenzhen; Fellow, CIGI

Akshay Mathur
Senior Fellow, CIGI

Rohinton P. Medhora
Distinguished Fellow, CIGI

Joshua P. Meltzer
Senior Fellow, Global Economy and Development, Brookings

Paul Samson
President, CIGI

Kendra Schaefer
Head of Tech Policy Research and
Partner, Trivium China

Shreeja Sen
Research Associate, IT for Change

Vikram Sinha
Head, Data Governance Network, IDFC Institute

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org