**Comparing the EU’s and China’s approaches in data governance**

Xuechen Chen[[1]](#footnote-1) and Xinchuchu Gao[[2]](#footnote-2)

**Abstract**

This chapter seeks to shed light on the following questions: to what extent is the EU a “good global actor” in the field of data governance? What are the limitations of the EU as a ‘willing-to-be’ good actor in data governance? Furthermore, what are the implications of other international actors’ competing approaches to data governance on the “goodness” of the EU’s role in this field? In order to reflect on these questions, this chapter takes into account inherent intensions existing in the EU’s data governance approach as well as implications of alternative approaches proposed by other actors in the field. It will be demonstrated that whilst there has been a strong willingness of the EU to act as a “good global actor” in data governance, its aspiration is limited by the dilemma of balancing data protection and technical innovation, or data protection and public interest as well as alternative approaches adopted by other major actors.

**Key words**: data governance, data protection, technical innovation, European Union, China, regulatory power

# Introduction

With the rapid development of information communications technologies (ICT), data governance has not only become one of the fastest-growing policy areas, but also has been regarded as a newly emerging battlefield for geopolitical competition among major international actors. As of January 2021, there were 4.66 billion active internet users worldwide, accounting for 59.5 percent of the global population.[[3]](#footnote-3) The rise of the data economy has been a major source of economic growth and technical innovation in recent decades. Meanwhile, cross-border data flows also present many risks, such as data misuse and abuse. Figuring out how to govern cross-border data flows therefore is becoming a priority for global policymakers. In January 2019, for instance, Japanese Prime Minister Shinzo Abe called for the G20 summit in Osaka to “be the summit that [starts] world-wide data governance”.[[4]](#footnote-4) Nevertheless, addressing these data-related issues at the global level is made hard by tremendous debates over how to balance protection and openness, or protection and innovation. Moreover, due to different understanding of how data should be stored, traded, and proceeded, different international actors have adopted divergent regulations on data governance, which has further generated policy challenges.

Against this backdrop, over the past few years the European Union (EU) has emerged as an increasingly crucial actor in the sphere of data governance, manifesting a strong ambition to strengthen its data governance regime internally as well as to exert greater influence in this field externally. Domestically, the EU has recently proposed a “Path to the Digital Decade”, a concrete action plan to achieve the digital transformation of European society and economy by 2030 with an aim to reinforce the EU’s digital sovereignty and digital leadership.[[5]](#footnote-5) Externally, the EU’s role as a rising regulation-setter in the digital sphere has gained increasing traction at international level, exemplified by the far-reaching implications of General Data Protection Regulation (GDPR) on transnational data governance as well as growing volume of literature evaluating the “Brussels Effect”.[[6]](#footnote-6) Nevertheless, despite the EU’s widely-accepted leadership role in data governance, the EU is constantly faced with the dilemma of balancing between protection and openness, or between protection and innovation. Meanwhile, the EU’s quest for leadership in data governance has been challenged by divergent visions and approaches adopted by other major international actors, such as the US and China.

In line with the theme of this book which interrogates the EU’s role as a good global actor, this chapter seeks to shed light on the following questions: to what extent is the EU a “good global actor” in the field of data governance? What are the limitations of the EU as a ‘willing-to-be’ good actor in data governance? Furthermore, what are the implications of other international actors’ competing approaches to data governance on the “goodness” of the EU’s role in this field? In order to reflect on these questions, this chapter takes into account inherent intensions existing in the EU’s data governance approach as well as implications of alternative approaches proposed by other actors in the field. It will be demonstrated that whilst there has been a strong willingness of the EU to act as a “good global actor” in data governance, its aspiration is limited by the dilemma of balancing data protection and technical innovation, or data protection and public interest as well as alternative approaches adopted by other major actors.

The past few years have witnessed the rise of China as an increasingly significant player capable of reshaping the norms and regulatory frameworks in global data governance.[[7]](#footnote-7) The EU’s and China’s data governance strategies differ greatly from each other not only in normative considerations and legal and regulatory frameworks, but also in terms of ways in which they exert influence beyond their borders. Nevertheless, there is relatively limited scholarly discussion that analyses the EU’s and China’s approaches to data governance through a comparative lens. Therefore, to bridge the gap of literature, this chapter offers a comparative analysis of the EU’s and China’s approaches to cross-border data governance.

Beyond this introduction, the chapter is divided into three sections. The first and second sections discuss the European and Chinese respective approaches to data governance, comparing the different underlying logics behind their approaches, policy instruments as well as their influence on global data governance. The final section examines the implications of the synergies and conflicts between the European and Chinese approaches to data governance on the EU’s approach and provides a conclusion.

1. **EU’s approach to data governance**

The EU is a major player in digital economy. The value of European data economy was about 301 billion euro (2.4% of GDP) in 2018. The same estimate predicts that it will increase to over 829 billion euros by 2025, representing 5.8 % of the overall EU GDP.[[8]](#footnote-8) The EU as a nascent yet important actor in data governance has been increasingly acknowledged in both policy and academic communities.[[9]](#footnote-9) One common argument is that the EU has become a regulatory power in the digital sphere, especially in transnational data governance.[[10]](#footnote-10) By launching numerous regulatory initiatives such as the Digital Single Market and the GDPR, the EU has increasingly been regarded as a regulation setter in privacy and data protection, given that many third countries have incorporated GDPR provisions in their national legislations.[[11]](#footnote-11) This line of argument has been reinforced by Bradford’s concept of “Brussels Effect”, which refers to the external impact of EU regulatory policies resulting from the EU’s externalization of its laws outside its borders through market mechanisms.[[12]](#footnote-12) The following paragraphs unpack the EU’s approach to data governance by illustrating the EU’s normative considerations behind its approach to data governance, policy instruments to manage transnational data, as well as its influence on global data governance.

*EU’s normative considerations on data governance*

The underlying logic of the EU’s data governance approach can be situated within a wider debate over the EU’s global role as a normative power. It has been widely argued that the EU sees itself as a benign global actor and a norm-promoter by placing a set of universal norms (e.g. peace, liberty, democracy, the rule of law, and respect for human rights) at the centre of its external relations with the rest of the world.[[13]](#footnote-13) The EU’s intention to act as a normative power is well reflected in the union’s approach to cross-border data governance. Remarkably, in the EU’s first cybersecurity strategy published in 2013, it is stressed that “the same norms, principles and values that the EU upholds offline, should also apply online” and that “fundamental rights, democracy, and the rule of law need to be protected in cyberspace”.[[14]](#footnote-14)

A cornerstone of the EU’s normative position on data governance is the protection of personal data and privacy.[[15]](#footnote-15) In the EU, privacy rights are given the status of a fundamental right that cannot be contracted away. Art. 8 of the 1950 European Convention of Human rights establishes the right of everyone to respect for their privacy.[[16]](#footnote-16) The 2009 Lisbon Treaty identifies data protection as a fundamental right.[[17]](#footnote-17) Meanwhile, the EU Charter of Fundamental Rights came into effect with the Lisbon Treaty, which affords individuals the right to the protection of their personal data.[[18]](#footnote-18) In the “European Data Strategy” published in 2020, the EU highlighted its commitment to “putting people first in developing technology, and defending and promoting European values and rights in the digital worlds”.[[19]](#footnote-19) By unveiling its strategies for data and Artificial Intelligence, the European Commission stressed that “Europe will continue to preserve its open, democratic and sustainable society and digital tools can support these principles. It will develop and pursue its own path to become a globally competitive, value-based and inclusive digital economy and society, while continuing to be an open but rules-based market, and to work closely with its international partners”.[[20]](#footnote-20)

Discussion above has illustrated that the EU has adopted a value-based vision and placed safeguarding fundamental rights such as privacy rights at the core of its approach to data governance. Nevertheless, the protection of data and privacy is arguably becoming a challenge for technical innovation and public interest in the EU. On the one hand, the European Commission has acknowledged that there exists the disconnect “big data innovation and privacy-aware data protection”.[[21]](#footnote-21) A telling example of this is the possible negative influence of the GDPR on the development and use of artificial intelligence (AI) in the EU. The EU has made it clear that it wants to play a leadership role in AI: “Overall, the ambition is for Europe to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI”.[[22]](#footnote-22) Given that access to and the ability to use data is a necessary prerequisite for the development and use of AI, law and regulations governing the use of data therefore will be the key factor in determining the EU’s pursuit of its leadership role in AI. The EU’s coordinated plan on AI has stated that, “AI needs vast amounts of data to be developed…The larger a data set, the better AI can learn and discover even subtle relations in the data”.[[23]](#footnote-23) However, social and economic benefits promised by the development of AI will remain largely untapped if data protection issues associated with it could not be addressed. One of the most direct restrictions in the GDPR that regulates the use of AI is the requirement in Article 22 that companies must manually review certain algorithmic decisions.[[24]](#footnote-24) This provision has significantly increased labor cost, therefore deterring the use of AI.[[25]](#footnote-25) Also, the GDPR is a complex piece of legislation. Companies that develop and use AI will need specialized personnel to follow the GDPR, thus raising the cost of AI and leading to a strong disincentive from using AI.[[26]](#footnote-26) In order to embrace the potential of data for the development and use of AI, more simplified EU regulations on data sharing are required.

On the other hand, with a focus on personal data protection, data access and sharing for public interest is arguably a neglected part of the EU’s data governance approach. Norms behind the EU’s approach to data governance are not limited to individual rights. Art. 2 of the Treaty on the EU, for instance, acknowledges collective rights that refer to economic conditions and societal relations, including equality, solidarity and tolerance.[[27]](#footnote-27) The European Court of Human rights has also held that a balance of individuals rights to the protection of data and privacy with collective rights is necessary in the application of Art. 8 ECHR.[[28]](#footnote-28) Nevertheless, in practice, data access and sharing for public interest is marginal in the EU.[[29]](#footnote-29) By the way of example, during the COVID-19 pandemic, processing personal health and genetic data for pandemic research in the EU has come across difficulties. The GDPR provides a legal basis for the processing of health data. However, the interpretation of public health provisions in the GDPR is left open to national legislatures. The resulting lack of legal clarity regarding public health provisions hampers the collection of data, which is valuable to address the pandemic.[[30]](#footnote-30) Moreover, the strict information-providing obligations under the GDPR have created an additional hurdle. According to the GDPR, research institutions have to provide extensive information on the purpose of data use before collection, including information on the legal basis for the processing of data and the intention to send data to third countries (Article 13). However, the implementation of these requirements may not be feasible when patients are in a serious state of illness.[[31]](#footnote-31) Observers therefore point out that learning from the COVID-19 crisis, the GDPR should clarify provisions regarding data access and sharing and provide legal certainty for researchers for public good.[[32]](#footnote-32)

*Policy instruments adopted by the EU’s data governance approach and their influence*

The EU has adopted a significant number of legal instruments to build its data governance regime. The GDPR, which was released in 2016, is the EU’s main piece of data regulation. The GDPR sets strict conditions on the handling of EU citizens’ personal data and asserts jurisdiction over the processing of European personal data, even in the case that citizen or data were physically outside of the EU. The publication of the GDPR turned the EU into a global leader in data protection.[[33]](#footnote-33) The GDPR was followed by its sister-regulation on the free flow of non-personal data (FFD) in 2018. In 2019, the EU released Cybersecurity Act[[34]](#footnote-34) and Open Data Directive.[[35]](#footnote-35) On 19 February 2020, the EU released its new Digital Strategy, composed of three documents that outline fundamental elements for the creation of Digital Europe. This package includes a five-year policy roadmap, a White Paper on Artificial Intelligence and European Data Strategy. The European Data Strategy data aims at “creating a single market for data that ensure Europe’s global competitiveness and data sovereignty”.[[36]](#footnote-36) Apart from the data protection regime, the EU seeks to arm itself with new powers against big tech firms.[[37]](#footnote-37) EU Internal Market Commissioner Thierry Breton stated that these new powers should include the ability to exclude large tech companies, such as Google and Facebook, from the European market if their dominance is deemed a threat to smaller firms or consumers.[[38]](#footnote-38) To achieve this goal, the EU passed the legislative proposal the Digital Services Act (DSA) and Digital Markets Act (DMA), which would increase responsibility and liability for social media firms and the content on their platforms.[[39]](#footnote-39)

Another example of the EU’s intention to build the data governance regime is its efforts on setting Artificial Intelligence regulations. Following the publication by the European Commission of the European strategy on AI in April 2018 and after extensive consultation, the High-Level Expert Group on Artificial Intelligence (HLEG) released Guidelines for Trustworthy AI in April 2019. This final report emphasized the importance of preserving human autonomy in the use of AI. In parallel, the Coordinated Plan on Artificial Intelligence (AI), first published in 2018, defined actions and funding instruments for the development of AI.[[40]](#footnote-40) The comprehensive update of the Coordinated Plan in 2021 takes into account of new challenges brought by the coronavirus pandemic and proposes concrete actions that are in line with the European Strategy on AI and the European Green Deal.[[41]](#footnote-41) Moreover, on 21 April 2021, the European Commission released its Artificial Intelligence Act (AIA). The AIA is the EU’s first-ever legal framework on AI and represents the EU’s most ambitious attempt to regulate AI technologies to date.[[42]](#footnote-42) It sets out a regulatory approach to the use of AI technologies across the European Union and its Single Market. Moreover, it will extend beyond the EU due to its extraterritorial scope: it applies to providers in third countries who place services with AI systems in the EU, as well as to providers whose AI systems produce outputs which are used in the EU.[[43]](#footnote-43)

To date, the EU has achieved much success in leveraging its influence in data governance at the global level. As acknowledged by research on European data sovereignty, being the first international actor to develop a regulatory framework for data protection has provided the EU with significant comparative advantage when promoting and externalizing its regulations. Given that the EU constitutes one of the largest and most developed consumer markets, large multinational corporations tend to accept compliance with the EU’s data protection obligations as the price for doing business in the EU. Since large transnational firms prefer streamline business operations, and therefore tend to voluntarily apply these EU regulations to their global operations so as to avoid the costs of adhering to multiple regulatory regimes. It can be observed that the EU’s Brussels Effect has contributed to reshaping multiple policy areas. For instance, large corporations such as Apple, Google, Facebook and Microsoft have decided to adopt one global privacy policy which mirrors heavily the EU’s GDPR.

In addition, the EU’s regulatory approach has been proven appealing to numerous third countries. For example, in the Asia-Pacific region, a number of new regulations and laws bear the hallmark of the EU’s GDPR. Established data protection regimes such as Australia, New Zealand and Singapore have drawn heavily from the GDPR.[[44]](#footnote-44) Another interesting example showing the EU’s ability to externalize its regulations can be found in the negotiation of the EU-Japan Economic Partnership Agreement (EPA). During the negotiation process, the EU maintained that data protection is a fundamental right in the EU and therefore is not up for negotiation.[[45]](#footnote-45) In order to obtain the reciprocal adequacy, Japan decided to implement additional safeguards and to put in place stricter regulations for the transfer of personal data. Following Japan’s remodeling of its data protection regulations, the EU and Japan eventually agreed to recognize each other’s data protection regimes in July 2018. These observations demonstrate that the EU has played an increasingly important role in shaping the regulatory environment in the field of data governance beyond its borders.

# China’s approach to data governance

Whilst the EU has been increasingly recognized as a leader in global data governance, there has been a growing consensus among public and academic debates that China has also emerged as a crucial player in transnational data governance, proactively seeking to reshape the regulatory environment and promoting its own approaches to data governance.[[46]](#footnote-46) Over the past few years, China has made great efforts to define its own data strategy and to reform its legal and regulatory frameworks of data governance at domestic level. Viewing data as “a new factor of production”[[47]](#footnote-47) and a “national strategic resource”[[48]](#footnote-48), Beijing seeks to build a comprehensive data governance regime as well as to establish a data market facilitating the growth of its digital economy. In the meanwhile, Beijing demonstrates greater ambition to act as a norm-entrepreneur and regulation-setter in global data governance through various instruments such as the Digital Silk Road[[49]](#footnote-49) and the Global Initiative on Data Security.[[50]](#footnote-50) Considering these dynamics, this sub-section examines China’s normative considerations and instruments concerning data governance, followed by a discussion on the influence of China’s quest for power and leadership on global data governance.

*China’s normative considerations on data governance*

Whilst the EU prioritizes a rights-based and value-driven data governance approach which attaches great importance to a set of EU norms such as human rights, privacy rights, gender digital equality and rule of law, China holds a fundamentally different normative position on data governance. Although China’s data governance regime has rapidly evolved over the past decade, it can be observed that Beijing’s normative consideration on data has primarily revolved around two different yet increasingly interconnected issues, namely national security and sovereignty, and economic development.

National security and sovereignty have long been Beijing’s key priorities when developing its data governance policies. Since the country’s opening to the Internet in the 1990s, China has adopted a security-centered approach to data governance, highlighting the importance of protecting the country’s digital infrastructure as well as countering cyberattacks and data leaks.[[51]](#footnote-51) In addition, in contrast with Western actors such as the US and the EU that call for a free and open global Internet, China emphasizes the norm of sovereignty in cyberspace and data governance, maintaining that sovereignty in cyberspace should be aligned to physical territorial boundaries of states.[[52]](#footnote-52) During a speech delivered at the World Internet Conference in 2015, Chinese president Xi Jinping highlighted the necessity to respect the sovereign equality of states in cyberspace and data governance, pointing out the risks of not allowing countries to govern their own cyberspace based on their own rules.[[53]](#footnote-53) The most comprehensive description of cyber sovereignty can be found in the International Strategy of Cooperation on Cyberspace issued in March 2017.[[54]](#footnote-54) This document emphasizes that the principle of sovereignty covers all aspects of state-to-state relations, which also includes cyberspace. Therefore, ‘countries should respect each other’s right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on equal footing’.[[55]](#footnote-55) The recently adopted Data Security Law reaffirms China’s normative considerations on national security and sovereignty. As indicated in a press release published by the State Council of China, from Beijing’s perspective, ‘the formulation of a data security law is an inevitable requirement for safeguarding national security. Data is a national strategic resource, and there is no national security without data security.’ [[56]](#footnote-56) It further stresses that the rationale behind the development of comprehensive data governance institutions is to protect and safeguard ‘national sovereignty, security and development interests’.[[57]](#footnote-57)

Whereas the consideration on national security and sovereignty remains as a focal point of China’s normative position on data governance, the past few years have witnessed an incremental shift in China’s narrative concerning data governance norms. Specifically, when examining Chinese official discourse, there has been increasing recognition of the necessity to balance the national security rationale to control data flows with economic imperatives to allow the creation of more fluid data sharing to benefit China’s digital economy and data markets.[[58]](#footnote-58) Therefore, it can be argued that, instead of being static and fixed, China’s normative consideration on data governance strategy has evolved over time, shifting from a logic that exclusively focused on national security and sovereignty to a more balanced approach that attaches equal importance to security and economic development. The Article 12 of China’s 2021 Data Security Law explicitly states that ‘the state firmly places equal emphasis on safeguarding data security and protecting data development and use’, implying that the adherence to the principles of data sovereignty and national security should go hand in hand with the creation of opportunities to use data to drive innovation and the digital economy.[[59]](#footnote-59) In addition, China’s State Council approved a plan to implement pilot comprehensive reform of market-based allocation of production factors in January 2022, which further reveals this transition in Beijing’s normative position on data governance. This newly published document aims to explore a new paradigm of trading data based on the idea that ‘original data should be stored within the territory of China and that data should be usable yet anonymized’.[[60]](#footnote-60) This new paradigm implies that China seeks to further balance its security and sovereignty-driven rationale and its desire to unleash the value of data resources.

*Policy instruments underpinning China’s data governance approach and their influence*

In comparison to the EU’s legislative framework of data governance, a systematic process of establishing a data governance regime in China is a more recent phenomenon. According to Liu, the formation of China’s cross-border data governance regime can be seen as part of the wider evolution of China’s Internet management system.[[61]](#footnote-61) Two crucial stages in the development of Chinese data governance regime can be identified. During the first stage (1994 – 2011), whilst there was a lack of a holistic approach to data governance in China, the legislative processes were heavily revolved around China’s concerns about outbound data security, focusing on the management of administrative affairs and national security issues, especially system security and state secrets. During this period, China produced a number of regulations and measures exemplified by the Security Regulations for Computer Information System (1994), the Decision of the NPC Standing Committee on the maintenance of Internet Security (2000). In the second stage (from 2011 onwards), China has attached more importance to establish regulatory measures for the local storage of data. Following the Snowden revelations in 2013, Chinese government accelerated the data security legislation, establishing provisions requiring data concerning the fields such as population health information, credit investigation, cloud services and Internet publishing services to be stored within China’s territory.[[62]](#footnote-62)

The Cybersecurity law, which was passed in November 2016, is China’s first comprehensive and fundamental law with regards to Internet governance, signifying that China’s cross-border data governance regime was finally implemented at the general legal level. Article 37 of the Cybersecurity Law stipulates that ‘Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China’, paving the way for the paradigm of ‘local storage and outbound assessment’ which lies at the core of China’s newly emerging data governance regime.[[63]](#footnote-63) Furthermore, in 2021, China’s Data Security Law and the Personal Information Protection Law, came into effect. These two new laws, along with the 2016 Cybersecurity Law, have laid the legal and institutional foundation for China’s evolving data governance system. At domestic level. Apart from the aforementioned basic laws, China’s data governance regime is also underpinned by a matrix of regulations and national standards, such as the latest draft of ‘Outbound Data Transfer Security Assessment Measures’ released in October 2021 and ‘Information Security Technology - Baseline for Cybersecurity Classification Protection’ issued in 2019.

Furthermore, in the past few years, China has taken an increasingly innovative approach to domestic data governance through initiating local pilot regulations on data and stakeholders’ public positions with a particular focus on corporate data rights and state-led data collection.[[64]](#footnote-64) One telling example is China’s first draft local regulation on data rights issued by the Standing Committee of People’s Congress in Shenzhen[[65]](#footnote-65), which explicitly defines three categories of data rights held by individual citizens, companies and the government. It is believed that this local regulation may serve as a potential blueprint for a national definition of data rights as well as a regulatory framework for data markets in China.[[66]](#footnote-66) Moreover, since the outbreak of the COVID-19, China has developed various new instruments to govern medical and healthcare data. For instance, since early 2020, Chinese governments started using a health code system to manage people’s movements in and out of affected areas. In December 2020, China has passed new guidelines on healthcare data security[[67]](#footnote-67) with an aim to define rights over medical and health data so as to establish a data regime which can both protect individual’s rights and incentivize effective data usage for public health purposes.

Apart from building its domestic data governance system, China is also playing an increasingly significant role in shaping the norms and rules in data governance at international level. Drawing on the recent studies on China’s role in transnational data governance and, more broadly, digital governance, the following paragraphs aim to unpack the mechanisms through which China exerts its influence in data governance beyond its borders. It will be shown that, in comparison to the EU’s normative and regulatory approach which prioritises the externalisation of EU-specific regulations and socio-political norms, China has exerted its influence through a different set of instruments.

It can be observed that China has leveraged its impact on data governance outside of its borders through the provision of digital infrastructures and technologies by Chinese companies, which may ultimately transform the conditions under which many developing countries develop their digital economies.[[68]](#footnote-68) Since 2013, China has made growing efforts to strengthen the external dimension of its digital strategy in order to ensure widespread adoption of Chinese technologies in third countries. In line with government directives to ‘go out’, Chinese government as well as high-tech companies have actively promoted Chinese technologies abroad. For instance, China attempts to expand its digital services and governing approaches through the launch of the Digital Silk Road (DSR) which forms part of the wider Belt and Road Initiative. This initiative seeks to expand digital infrastructure, promote digital service and e-commerce, as well as develop common digital technology standards amongst participating countries. Notably, China published a white paper in 2015 which explicitly made digital connectivity a top priority.[[69]](#footnote-69) The DSR not only aims to offer support to Chinese exporters (including tech companies) but also seeks to improve the recipient countries’ telecommunications infrastructures and networks, AI capabilities, e-commerce, surveillance technologies and other technology areas.[[70]](#footnote-70) A large number of countries in the global south, including countries in Africa, the Middle East, Latin America, and Southeast Asia demonstrate growing interest in participating in the DRS projects by signing agreements and MOUs with China due to their increasing demand for high-quality technology and telecommunication infrastructures.[[71]](#footnote-71) Through these initiatives, China has acquired new opportunities to leverage its influence in transnational data governance beyond its territory. DRS-related investments and projects not only allow China to provide critical ICT infrastructure in participant countries, but also facilitate technical knowledge transfer in many areas through cooperation between engineers and scientists.[[72]](#footnote-72) By doing so, China exerts its influence on global data governance through transforming the conditions under which developing countries transition into digital economies.[[73]](#footnote-73) Furthermore, China has played a proactive role in initiating and participating in multilateral platforms to promote its vision on data governance. For example, in 2020, China announced a new multilateral platform – ‘Global Initiative on Data Security’ – to articulate its vision and approach to data governance. Through this initiative, Beijing seeks to promote its own norms on data security which is based on strong data localization requirements by emphasizing the importance for different countries and jurisdictions to govern data and their digital economies as they wish according to the principle of mutual respect.[[74]](#footnote-74)

In addition, China’s relatively successful performance in managing the Covid-19 infections is closely linked to China’s massive collection and processing of individual data, which may further encourage other countries to follow suit.[[75]](#footnote-75)

# Implications on the EU’s role as a good global actor in data governance

Discussion above has illustrated that the EU’s data governance approach differs from the one adopted by China in three ways. Firstly, the EU has prioritized data and privacy protection as the principal norm driving its data governance approach whereas China’s normative consideration on data has primarily revolved around two different yet increasingly interconnected issues, namely national security and sovereignty, and economic development. Secondly, the EU has leveraged its impact on global data governance mostly through legal instruments, namely the publication of initiatives, regulations and laws, while China has promoted its data governance approach through the provisions of digital infrastructures and technologies by Chinese companies. Thirdly, with regard to their influence, the EU’s data governance approach, its data protection regulations in particular, has been widely accepted worldwide. In contrast, the external influence of China’s data governance remains limited. Nevertheless, Chinese approach has recently started gaining increasing traction among a number of countries from the Global South who participated in China’s Digital Silk Road.

The implications of the synergies and conflicts between the European and Chinese approaches to data governance on the EU’s role as a ‘good global actor’ could be understood from a twofold perspective. Firstly, the EU needs to address the tension between the requirements of data protection and the necessity to unleash the value of data so as to ensure technical innovation and public interests.

As discussed earlier, although consideration of national security and sovereignty remains as a focal point of China’s normative position on data governance, China has increasingly attached more importance to economic development when developing its approach to data governance. Consequently, the past few years have witnessed the rapid development of data market in China. Europe is arguably lagging behind China in data technology and economy.[[76]](#footnote-76) There are limited number of big tech companies in the EU than in the U.S. and China. Of the 603 currently listed high-growth unicorn companies, defined as a private company with a valuation over $1 billion, only 41 are based in the EU, while 298 are based in the U.S. and 140 are based in China.[[77]](#footnote-77) Therefore, in order to exploit the economic potential of data and to become a more competitive actor in global data governance vis-à-vis China and the US, the EU should address the tension between its emphasis on data and privacy protection and economic imperatives.

Secondly, the EU needs to reduce its reliance on Chinese cloud and data infrastructure to preserve its autonomy in data governance. Although the EU has achieved much success in leveraging its influence in data governance globally through the adoption of legal instruments, its data governance approach is challenged by policy instruments adopted by China. China’s data governance approach has increasingly emerged as an attractive alternative to developing countries, as evidenced in the expansion of China’s Digital Silk Road initiative. Specifically, China’s supply of digital technologies and infrastructure in third countries play an important role in transforming the conditions under which many developing countries develop their digital economies and data governance frameworks. As a result, in order to leverage greater external influence, the EU should go beyond its prioritization of the use of legal instruments and attach more importance to the provision of digital technologies and infrastructure beyond its borders.

In conclusion, this chapter investigates the EU’s role as a good global actor through a comparative analysis of the EU’s and China’s approaches to data governance, with a focus on examining normative considerations behind their approaches, policy instruments as well as their influence on global data governance. The chapter maintains that, whereas the EU had held a strong wiliness to act as a good global actor in data governance, its aspiration is limited by an inherent tension between the requirements on the one hand to protect data and privacy, and on the other hand do so without creating addition hurdles to achieving technical innovation and protecting public interest. Moreover, the EU’s quest for leadership in data governance has been challenged by the divergent approach adopted by China.

1. Faculty of Politics and International Relations, New College of the Humanities at Northeastern University [↑](#footnote-ref-1)
2. European Institute, London School of Economics [↑](#footnote-ref-2)
3. Statista (2021). *Global digital population as of January 2021*, available at <https://www.statista.com/statistics/617136/digital-population-worldwide/>, accessed on 06 January 2022. [↑](#footnote-ref-3)
4. World Economic Forum (2019). *Defeatism about Japan is now defeated: Read Abe’s Davos speech in full*, available at <https://www.weforum.org/agenda/2019/01/abe-speech-transcript/>, accessed on 10 January 2022. [↑](#footnote-ref-4)
5. European Commission (2021). *State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU’s digital transformation by 2030*, available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630>, accessed on 08 January 2022. [↑](#footnote-ref-5)
6. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA; Bygrave, L. A. (2021). *The ‘Strasbourg Effect’ on data protection in light of the ‘Brussels Effect’: Logic, mechanics and prospects*. Computer Law & Security Review, 40. [↑](#footnote-ref-6)
7. See for example Sacks, S., Triolo, P., & Webster, G. (2017). Beyond the worst-case assumptions

   on China’s cybersecurity law: There’s still an internal tug-of-war over cross-border data flows. New America; Liu, J. (2020). China’s data localization. Chinese Journal of Communication, 13(1), 84-103; Erie, M. S., & Streinz, T. (2021). The Beijing Effect: China's' Digital Silk Road'as Transnational Data Governance. New York University Journal of International Law and Politics (JILP). [↑](#footnote-ref-7)
8. European Commission (2020). *Final Study Report: The European Data Market Monitoring Tool Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories.* available at: https://datalandscape.eu/sites/default/files/report/D2.9\_EDM\_Final\_study\_report\_16.06.2020\_IDC\_pdf.pdf, accessed on 12 June 2021. [↑](#footnote-ref-8)
9. Liaropoulos, A. (2021). EU Digital Sovereignty: A Regulatory Power Searching for its Strategic Autonomy in the Digital Domain. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (p. 246). Academic Conferences Inter Ltd.; Dunn Cavelty, M. (2018). Europe's cyber-power. *European Politics and Society*, *19*(3), 304-320; [↑](#footnote-ref-9)
10. Liaropoulos, A. (2021). EU Digital Sovereignty: A Regulatory Power Searching for its Strategic Autonomy in the Digital Domain. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (p. 246). Academic Conferences Inter Ltd. [↑](#footnote-ref-10)
11. Madiega, T. (2020). *Digital sovereignty for Europe* (Briefing PE 651.992; EPRS Ideas Papers). European Parliamentary Research Service. [↑](#footnote-ref-11)
12. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA. [↑](#footnote-ref-12)
13. Manners, I. (2002). Normative power Europe: a contradiction in terms?. *JCMS: Journal of common market studies*, *40*(2), 235-258; Whitman, R. (Ed.). (2011). *Normative power Europe: Empirical and theoretical perspectives*. Springer. [↑](#footnote-ref-13)
14. European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, p.2. [↑](#footnote-ref-14)
15. European Commission (2019). Data Protection Rules as a Trust-enabled in the EU and beyond—taking stock, Brussels, COM(2019) 374 final. [↑](#footnote-ref-15)
16. European Parliament (2021). *Fact Sheet on the EU: Personal Data Protection*, available at <https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection>, accessed on 12 January 2022. [↑](#footnote-ref-16)
17. Treaty on the Functioning of the European Union, Art. 16, 2012 O.J. 9C326) [↑](#footnote-ref-17)
18. Charter of Fundamental Rights of The European Union, arts. 7-8, 2007 O.J. (C303) 1 [↑](#footnote-ref-18)
19. European Commission (2021). *A European Strategy for Europe*, available at <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>, accessed on 12 January 2022. [↑](#footnote-ref-19)
20. European Commission (2020). *Shaping Europe’s digital future: Commission presents strategies for data and Artificial Intelligence*, available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273>, accessed on 11 January 2022. [↑](#footnote-ref-20)
21. European Commission (2021). *Bridging the divide between big data innovation and privacy-aware data protection*, available at <https://cordis.europa.eu/article/id/428905-bridging-the-divide-between-big-data-innovation-and-privacy-aware-data-protection>, accessed on 11 January 2022. [↑](#footnote-ref-21)
22. European Commission (2018), *Coordinated Plan on Artificial Intelligence*, available at <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence>, accessed on 12 January 2022. [↑](#footnote-ref-22)
23. Ibid. [↑](#footnote-ref-23)
24. European Union (2016), General Data Protection Regulation (GDPR), Article 22. [↑](#footnote-ref-24)
25. Nick Wallace and Daniel Castro (2018), “The Impact of the EU’s New Data Protection Regulation on AI, available at <http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf>, accessed on 06 January 2022. [↑](#footnote-ref-25)
26. Ibid. [↑](#footnote-ref-26)
27. European Union (1993). Treaty on the European Union. [↑](#footnote-ref-27)
28. European Union (2012). The European Convention on Human Rights, Article 8. [↑](#footnote-ref-28)
29. Kerber, W. (2017). Rights on data: The EU communication “Building a european data economy” from an economic perspective. In Lohsse, S. (Ed.), *Trading data in the digital economy: Legal concepts and tools*. Hart Publishing. [↑](#footnote-ref-29)
30. Becker, R.,Thorogood, A., Ordish, J. & Beauvais, Michael J. S. (2020). *COVID-19 Research: Navigating the European General Data Protection Regulation*, Journal of Medical Internet Research 22(8): e19799 [↑](#footnote-ref-30)
31. *Ibid.* [↑](#footnote-ref-31)
32. Christofidou, M., Lea, N., & Coorevits, P. (2021). A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection during a time of Crisis. *Yearbook of medical informatics*, *30*(01), 226-232. [↑](#footnote-ref-32)
33. Schwartz, P. M. (2019). *Global data privacy: The EU way*. NYUL Rev., 94, 771. [↑](#footnote-ref-33)
34. European Union (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [↑](#footnote-ref-34)
35. European Union (2019). Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. [↑](#footnote-ref-35)
36. European Commission (2021), A European Strategy for data, available at <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>, accessed on 11 January 2022. [↑](#footnote-ref-36)
37. Espinoza, J. and Fleming, S. (2020). EU seeks new powers to penalise tech giants, Financial Times, available at <https://www.ft.com/content/7738fdd8-e0c3-4090-8cc9-7d4b53ff3afb>, accessed on 08 January 2022. [↑](#footnote-ref-37)
38. Hellard, B. (2020). *EU Seeks to New Regulatory Powers against Big Tech Firms: powers could include the ability to exclude large tech companies from the Single Market altogether*, ITPro., September 21, available at <https://www.itpro.co.uk/business/policy-legislation/357172/eu-seeks-new-regulatory-powers-against-big-tech-firms>, accessed on 06 June 2021. [↑](#footnote-ref-38)
39. European Commission (2019). *The Digital Services Act: ensuring a safe and accountable online environment*. available at <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en>, accessed on 11 June 2021. [↑](#footnote-ref-39)
40. European Commission (2021). *Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence*, available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682>, accessed on 06 June 2021. [↑](#footnote-ref-40)
41. Ibid. [↑](#footnote-ref-41)
42. European Commission (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence,* available at <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>, accessed on 06 June 2021. [↑](#footnote-ref-42)
43. Centre for Data Ethics and Innovation, UK (2021). *The European Commission’s Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem*, available at <https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/>, accessed on 06 June 2021. [↑](#footnote-ref-43)
44. # Hogan Lovells (2020), Hogan Lovells Asia Pacific Data Protection and Cyber Security Guide 2020, available at <https://www.hoganlovells.com/en/publications/hogan-lovells-asia-pacific-data-protection-and-cyber-security-guide-2020>, accessed on 11 January 2022.

    [↑](#footnote-ref-44)
45. Kanetake, M. and de Vries, Sybe (2018). *EU-Japan Economic Partnership Agreement: Data Protection in the Era of Digital Trade and Economy*, RENFORCE BLOG, available at <http://blog.renforce.eu/index.php/en/2018/12/18/eu-japan-economic-partnership-agreement-data-protection-in-the-era-of-digital-trade-and-economy/>, accessed on 11 January 2022. [↑](#footnote-ref-45)
46. See for example Erie, M. S., & Streinz, T. (2021). The Beijing Effect: China's' Digital Silk Road'as Transnational Data Governance. New York University Journal of International Law and Politics (JILP); Kak, A and Sacks S. (2021). Shifting Narratives and Emergent Trends in Data-Governance Policy, Yale Law School; Boullenois, C. (2021). China’s data strategy: creating a state-led market. EUISS. [↑](#footnote-ref-46)
47. Ouyang, S. and Chen, J. (2020). New Guideline to better allocate production factors, *China Daily,* available at: <https://www.chinadaily.com.cn/a/202004/10/WS5e903fd7a3105d50a3d15620.html> [↑](#footnote-ref-47)
48. Reuters, (2021). China seeks better cross-border control of big data, available at: <https://www.reuters.com/technology/china-urges-stronger-cross-border-security-big-data-2021-11-30/> [↑](#footnote-ref-48)
49. Erie, M. S. & Streinz, T. (2021). [↑](#footnote-ref-49)
50. Tiezzi, S. (2020). China’s bid to write the global rules on data security. *The Diplomat*. Available at: <https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/> [↑](#footnote-ref-50)
51. Boullenois, C. (2021). China’s Data Strategy. EUISS. [↑](#footnote-ref-51)
52. Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. In 4th USENIX Workshop on Free and Open Communications on the Internet; Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: the case of China. Chinese Journal of Communication, 13(1), 8-26. [↑](#footnote-ref-52)
53. Xinhua Net (2015), Speech by Xi Jinping at the Opening Ceremony of the Second World Internet Conference, available at [http://www.xinhuanet.com//politics/2015- 12/16/c\_1117481089.htm](http://www.xinhuanet.com//politics/2015-%2012/16/c_1117481089.htm) [↑](#footnote-ref-53)
54. Ministry of Foreign Affairs of the People’s Republic of china (2017), International Strategy of cooperation on Cyberspace, available at <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml> [↑](#footnote-ref-54)
55. Ibid. [↑](#footnote-ref-55)
56. The State Council of China. (2021). Data Security Law: Safeguarding Data Security and Helping the Development of the Digital Economy, available at: <http://www.gov.cn/xinwen/2021-06/10/content_5616847.htm> [↑](#footnote-ref-56)
57. Ibid. [↑](#footnote-ref-57)
58. Kak, A. and Sacks, S. (2021). Shifting narratives and Emerging Trends in Data Governance Policy. Yale Law School. Available at: <https://law.yale.edu/sites/default/files/area/center/china/document/shifting_narratives.pdf> [↑](#footnote-ref-58)
59. Ibid. [↑](#footnote-ref-59)
60. State Council of China (2021). A plan to implement pilot comprehensive reform of market-based allocation of production factors. Available at: <http://www.gov.cn/zhengce/content/2022-01/06/content_5666681.htm?trs=1> [↑](#footnote-ref-60)
61. Liu, J. (2020). China’s data localization. Chinese Journal of Communication, 13(1), 84-103. [↑](#footnote-ref-61)
62. Ibid. [↑](#footnote-ref-62)
63. Ibid. [↑](#footnote-ref-63)
64. Boullenois (2021) [↑](#footnote-ref-64)
65. the Standing Committee of People’s Congress in Shenzhen (2021) Data Regulations of Shenzhen Special Economic Zone (the Shenzhen Data Regulation), available at: <http://www.sz.gov.cn/szzsj/gkmlpt/content/8/8935/post_8935483.html#19236> [↑](#footnote-ref-65)
66. Boullenois (2021) [↑](#footnote-ref-66)
67. National Information Security Standardization Technical Committee, Health and Medical Data Security Guidelines, March 2021 (https://www.shangyexinzhi.com/article/3421609.html). [↑](#footnote-ref-67)
68. Erie and Streinz, (2021) [↑](#footnote-ref-68)
69. National Development and Reform Commission of China, Vision and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road (March 2015). [↑](#footnote-ref-69)
70. Kurlantzick, J, “China’s digital silk road initiative: a boon for developing countries or a danger to freedom?”, The Diplomat (December 2020), available at: <<https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/>>, accessed 16 June 2021. [↑](#footnote-ref-70)
71. Ibid. [↑](#footnote-ref-71)
72. Ibid. [↑](#footnote-ref-72)
73. Erie and Streinz, 2021 [↑](#footnote-ref-73)
74. MERICS, (2020). China’s global initiative on data security has a message for Europe. Available at: <https://merics.org/en/analysis/chinas-global-initiative-data-security-has-message-europe> [↑](#footnote-ref-74)
75. Boullenois, (2021). [↑](#footnote-ref-75)
76. Amiot, E., Palencia, I. Baena, A. and de Pommerol, C. (2020). *European Digital Sovereignty: Syncing Values and Value*, available at <https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html>, accessed on 11 June 2021. [↑](#footnote-ref-76)
77. CBINSIGHTS (2021). The Complete List of Unicorn Companies, available at <https://www.cbinsights.com/research-unicorn-companies>, accessed on 06 June 2021. [↑](#footnote-ref-77)