CHERN POLICY BRIEF 2021/02
December 2021

Fragmented Global Data Governance:
the Role of China, the EU, and the US

Already in 2006, a British mathematician Clive Humby, coined the phrase "Data is the new oil". While a flawed statement, as data is infinitely renewable and can be utilised in multiple ways, this statement does reflect well the high value attached to data as a driver of economic growth and innovation. Today, the importance of data is still more valid than ever, especially with the COVID-19 pandemic putting more pressure on the digital realm. Governments, businesses, and citizens were forced to continue their work online, creating a hasty adoption of digital means that is unlikely to reverse. Data has thus emerged as a force of change in all facets of societal life, which spurred the debate on global data governance. It calls for better understanding of whether and how countries are using legal rules to handle data usage and the geopolitical implications of these rules.

Key recommendations

- Considering China's game-changing data laws and regulation, the EU should avoid perpetuating a fragmented global data governance that contribute to data protection, interoperability problems and international trade barriers by combining a top-down and bottom-up political approach and regulation.
- The EU needs to support small and medium-sized entrepreneurs' (SME) growth because fragmented data regimes possess high risks to SMEs, especially with the rise and presence of large US' and Chinese global tech champions.
- The establishment of a multidisciplinary multinational expert working group, independent from political and private interests, could provide indication as to the present and future constrains upon regulatory cooperation.

Data is information, collected, stored, and used in an electronic form. The European Union (EU) and People's Republic of China (PRC) have a different approach towards data. For the EU, regulation of personal data – data is directly or indirectly relating to an identified or identifiable natural person – is the primary focus under the General Data Protection Regulation (GDPR). With a data strategy of balancing individual data protection and flexibility to allow for the legitimate interests of the business and the public, the EU is positioning itself in the data governance debate. In the Chinese context, data was defined as "an important basic strategic resource for the country" in the 13th Five-Year Plan and the Big Data Industry Development Plan. The definition and classification criterion involve personal information, personal sensitive information, important data, state secrets, and other special data with industry characteristics such as human genetic resources. The legislation includes this terminology.

cost EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY
Funded by the European Union
CHERN China in Europe Research Network CA18215
https://china-in-europe.net/

Differences in approaches to global data governance exist, which raise the question of what are the implications for the EU's digital transformation and for a global data governance. This policy brief will first highlight the present global data governance. It will then outline the European approach, whereafter it will elaborate upon China's data governance regime. The differences between China's and the EU's approaches will be discussed, including some references to the United States' (US) approach, and the convergence that can be found. This policy brief will discuss the divergences between China's and PRC cyber and data governance conceptualisations. Lastly, it will present policy recommendations.

The risks to fragmented global data governance

Global data governance is reshaping relations between governments, businesses, citizens, and consumers. From a private sector perspective, innovation, productivity, and competitiveness depend on how companies can leverage data, exploit digital services and goods, and navigate between regulatory frameworks and jurisdictions. Today, Alphabet (Google), Amazon, Apple, Facebook, and Microsoft (often referred to as GAFAM) are still the dominant global players, all head-quartered in the US. In the last five years, Chinese tech giants have made their entrance on the global digital market next to the US companies, including but not limited to companies such as Huawei, Xiaomi, ByteDance, Tencent, and Alibaba. European tech firms have been trying to compete with these US and Chinese businesses, but are frequently having trouble competing in the global market. These tech firms use AI applications, such as machine learning systems or chat bot assistants, which require large volumes of data, variety of data, and data quality and veracity. Platforms, in particular social networking sites, are an example of data being exploited, for commercial purposes and for global standard setting. Platforms create sophisticated systems of private governance that regulate users arbitrarily and without due process, transparency, and accountability. Oftentimes the incentives for this tangle of arbitrary rules are the competing legal rules for platforms in different jurisdictions. Hence, consumers are highly vulnerable to digital surveillance and manipulation, including fake news, echo chambers, and being banned from a platform without prior notice or warning.

The dependency on and importance of data has brought concerns about data collection and data use and the privacy of citizens. It also exposed differences in data regulatory frameworks, in particular between the EU, US, and PRC. Different approaches have led to divergences in the legal instruments used and the level of protection afforded to individuals, with a notable distinction between privacy from the government and from the private sector.

The US has prioritised the interests of businesses, with a strong focus on protecting citizens' privacy from the state but not from the private sector. There is no federal law covering all aspects of data privacy, but a jumble of several laws enacted on both federal and state level have been developed to protect citizens data, thereby offering less protection to consumers as a result of data use by companies. Only specific sectors are subject to federal statutes, such as financial services and healthcare. US-based companies benefit from this environment as they can strengthen their competitive advantage by collecting and using consumers' data to further develop digital goods and services without much pushback. Nevertheless, as visualised in Figure 1, there is no equidistance between the transatlantic relationship on data governance and the China-EU relationship on data

governance. While the EU and US differ strongly on the regulation for Big Tech companies, they do have a potential for a global tech alliance, as is reflected in the talks on the Transatlantic Trade Tech Council.

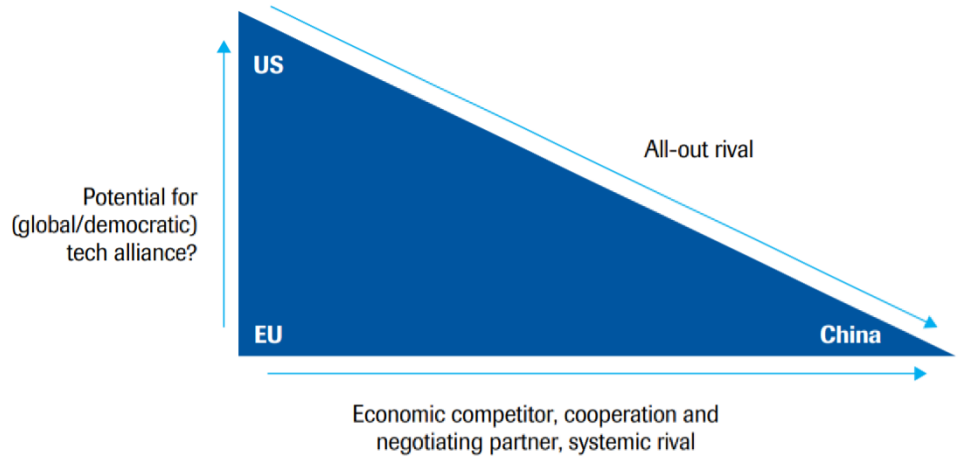


Figure 1

No equidistance: the transatlantic relationship and the EU/US views on China in trade-tech issues reflected in a scalene triangle

Source: Dekker, B. and Okano-Heijmans, M. (2020)

China's approach, by contrast, targets unlawful use of personal information by non-state actors. Regulators have shifted to a more stringent data regime, protecting consumers, which bear a resemblance to the EU's approach to personal data protection and surpasses US legislation. Nonetheless, the government is able to access data without any safeguards when deemed necessary for public and national security. Yet, like US law enforcement, policies prioritise national security over the rights and freedoms of data subject, which has been the main raison for the Court of Justice of the European Union (ECJ) to invalidate the EU-US Privacy Shield (publicly known as the *Schrems II* ruling). It was deemed invalid – striking down the EU-US Safe Harbor agreement – by alleging concerns about the US government access to personal data of Europeans. The EU represents a third way, emphasising the right to privacy and personal data protection as fundamental rights, a human-centred approach that puts citizens first and includes a strong focus on values and ethics. This, however, also includes additional challenges for EU-based companies and global companies handling EU-data, as they have to adhere to the EU data protection rules.

That said, domestic regulations concerning privacy protection, store-collect-use of data, ownership, and national security do constitute a detrimental impact on economic and trade issues. Data protectionism is on the rise; from 35 countries having localisation restrictions in 2017 to 62 countries imposing 144 restrictions in 2021 – among those, the PRC, India, and Vietnam. States seek to localise data flows so as to ensure jurisdictional control and enforceability of national rules applying to national/data sovereignty concepts. Consequently, data regimes fragmentation and interoperability obstacles exist, showing an upward trend that is expected to continue. Eventually, these fragmentated regulatory approaches could lead to a bifurcation of the internet as such.

The EU's take on data governance and its limits

The EU is considered a frontrunner in data governance regime with the adoption of the General Data Protection Regulation (GDPR) in 2016. As part of the EU's digital strategy, the Commission also adopted Regulation on Data Governance (2020). This proposal complements the existing strategies, programmes, and plans such as *Data Strategy*, *New Industrial Strategy, AI White Paper,* Digital Europe Programme (2021-2027), *Single Market Enforcement Action Plan*, and *Digital Services Act Package*. The EU also shows the political determination to shape data governance in Europe and beyond with the implementation of projects like the Franco-German Gaia-X initiative and Open Science Cloud programs.

Reality, however, casts serious doubts on the EU's ability to achieve its goal to be a norm and standard setter in the digital sphere, and particularly in setting a global data regime. Due to a poor start-up ecosystem, the low number of tech-champions, limited funding, and the absence of a well-developed digital business market, evidence the European commercial and security weaknesses. In addition to this, supranational structural limitations and Member States' (MS) divergent interests observed in digital taxation or even in the implementation of the 5G Toolbox, reflect internal challenges between MS before the EU can confidently act as an international norm- and standard setter in the digital domain.

Recognising these imperfections, for the EU and its MS, the digital internal market priorities are threefold: data, economy, and secure environment for digital networks and services. In this regard, the European *Data Strategy* aims to increase trust in data sharing across MS and sectors, strengthen mechanisms to increase data availability, and overcome technical obstacles. The data strategy intends to ensure more control for citizens and companies over the data they generate. Additionally, it pursues to strengthen the protection of information space, which is dominated by non-European geoeconomic players, and establish the legal framework for a single data space. The EU will invest €2 billion in a High Impact Project to develop data processing infrastructures, data sharing tools, architectures and governance mechanisms for thriving data sharing, to federate energy efficient, and trustworthy cloud infrastructure and related services.

Following the global trend of linking data privacy, ownership, and sovereignty risks, scholars and policy-makers acknowledge that Big Data also bring security issues regarding privacy protection laws requiring transparency and user consent, and data minimisation. This global trend also shows within the EU that various MS, such as Germany, Italy, France, the Netherlands, Sweden, and Poland, have data localisation requirements in place. Localisation can be considered a market protectionism measure rather than a protection principle for citizens' rights. For example, in Germany, telecommunications metadata, financial bookkeeping records, VAT invoices, and accounting records need to be stored locally giving an advantage to those companies that can store their data locally. Fragmentation of digital space and legal regimes that prevent free flow of data could impact the growth of the data-driven economy. Overregulation in a data protection regime could create greater costs than benefits for companies, particularly SMEs. At the international level, the current primary example showing tensions between the transatlantic partners on the balance between data protection, trade, economic competitiveness, and security matters is the invalidation of the EU-US Privacy Shield by the ECJ.

Understanding cyber and data sovereignty in Europe

The European Union Charter of Fundamental Rights stimulates that all EU citizens have the right to protection of their personal data. In order to 'make Europe fit for the digital age', the data protection package has been adopted in 2016. Regulation (EU) 2016/679 has been part of this package and is better known as the General Data Protection Regulation (GDPR). The GDPR aims to protect citizens regarding the processing of their personal data and on the free movement of their personal data between the EU MS and beyond. Personal data under the GDPR refers to any information relating to an identified or identifiable natural person ('data subject'). Any information is a rather broad and inclusive term, and includes objective information such as a citizens' height but also subjective information such as evaluations. The GDPR applies to personal data processed in automated means – such as electronic forms – or processed in a non-automated manner.

The regulation entered into force in 2016 and applies to all EU MS since May 2018. This regulation is unique as one single law has been applied to all EU countries and companies in and outside of the EU that handle EU-citizens data. The ultimate aim of this regulation was to remove fragmentation in the MS and avoid any unnecessary administrative burdens. The European Data Protection Board (EDPB) ensures the consistent application of data protection rules in the MS. It is an independent body composed of national data protection authorities representatives and of the European Data Protection Supervisor. The European Commission is an active member without voting rights.

China's evolving data governance regime

As data has become a geopolitical matter, it is important to understand the data governance regime of one of the rising global tech players next to the US. In September 2020, only seven months after the publication of the *European Data Strategy* and allegedly as a response to the US Clean Network Programme – a US initiative to protect 5G networks from untrusted vendors – China announced its *Global Data Security Initiative*: an attempt to introduce an alternative to the Western-led rules-based order on data governance. In general, the Initiative introduced multilateralism, the development of security and fairness, and justice as the most important pillars.

Still today, China's data governance regime is constantly evolving. There is no one all-encompassing law in the PRC, instead, a collection of legislation, measures, and standards conform the data protection framework. In addition, national strategies and plans play crucial roles to pursue the PRC strategic aim to become self-sufficient and a global tech leader. The legislation classification regarding China's data governance regime has been visualised in Table 1. At present, China has not developed legal instruments to influence other regimes; however, through digital infrastructure projects and tech companies providing services abroad Chinese companies could exert an indirect influence. The counterbalance of this potential influence will depend on domestic legal and political systems of receptors jurisdictions.

Figure 2 (next page)

China's legislation classification regarding data governance regime

Note: The most important laws that have been passed are marked bold

Laws

2021 Nov. Personal Information Protection Law
2021 Sept. Data Security Law
2021 Jan. Civil Code
2021 Jan. Encryption
2019 Jan. E-Commerce
2018 Jan. Standardisation (revised 1989 Standardisation Law)
2017 Oct. General Provisions of the Civil Law
2017 Jun. Cybersecurity Law
2016 Jan. Counter-Terrorism
2015 Nov. Criminal Law [Amend IX]
2015 Jul. National Security
2015 Mar. Criminal Law [Amend IX]
2014 Mar. Consumer Rights Protection
2012 Dec. Decision on Strengthening Online Information Protection
2012 Oct. State Secrets Protection Law
2010 Jul. Tort Liabilities Law
2004 Jan. Resident Identity Card Law

Regulations and measures

Regulations

2021 Oct. Security of Automobile Data (for trial implementation)
2020 Feb. Technical Specification for Personal Financial Information Protection
2020 Apr. Guide for health data security
2020 March Guide for de-identifying personal information
2019 Dec. Cybersecurity Multi-Level Protection Regulations
2018 April Administration of Scientific Data
2016 Nov. Online Taxi Booking Business Operations and Services
2015 Mar. Account Names of Internet Users Administration Regulations
2014 Administration of Population Health Information (trial)
2013 Sept. Telecommunications and Internet User Personal Information Protection Regulations
2013 Mar. Administration of Credit Investigation Industry
2012 Mar. Several Provisions on Regulating the Market Order of Internet Information Services

Measures

2021 Sept. Security Protection of Critical Information Infrastructure
2021 Jan.* Regulatory Data Security (for Trial Implementation)
2020 Nov. Protection of Financial Consumers' Rights and Interests
2019 June* Measures for Personal Data Cross-Border Transfer Security Assessments
2019 May* Data Security Management (draft)
2019 June* Security assessment of the overseas transfer of personal information and important data (draft)
2017 April* Security Evaluation of Cross-Border Personal Information and Important Data (Draft – Comments)
2007 June Measures for the Multi-level Protection of Information security

GB National Standards

2021 Jun. Guidelines on Personal Information Security Impact Assessment
2021 April Financial data security: Security specification of data life cycle
2020 Oct. Personal Information Security Specification (PIS Specification)
2020 Sept. Interpretation of the Cybersecurity Multi-Level Protection Regulations 2.0
2020 Apr. Guide to the construction of network data security standard system (draft)
2017 Aug.* Security Technology Guidelines for Data Cross-Border Security Assessment
2013 Feb. Guidelines for the protection of personal information protection within information system for public

Guidelines

2021 March Cybersecurity Standard Practice Guide: Guidelines for personal information security protection of mobile internet applications
2020 Sept. Financial Data Security—Guidelines for Data Security Classification
2020 July Self-assessment guidelines for Apps to collect and use personal information
2019 Apr. Internet Personal Information Security Protection
2019 March Guide to the self-assessment of illegal collection and use of personal information by apps
2018 Data Management of Banking Financial Institutions
2018 Jan.* Guidelines for data cross-border transfer security assessment
2017 Aug.* Data Cross-Border Transfer Security Assessment [Draft]

Provisions

2021 Apr. Scope of necessary personal information for common types of mobile internet applications [draft]
2021 March Protection and management of personal information in Mobile Internet Applications (draft)
2018 Oct. Online Protection of Children's Personal Information
2018 May. Personal Information Security Specification
2017 Sept. Criminal cases involving infringement of citizens' personal information
2016 Aug. Administration of Mobile Internet Applications Information Services
2013 Sep. Protection of personal information of telecoms and internet users

Notices

2019 Nov. Promulgation of the method for identifying the illegal collection and use of personal information by apps
2018 Nov. Determination of the collection and use of personal information by Apps in violation of laws and regulations
2011 Urging banking financial institutions to do a good job in protecting personal information

* Is not effective yet, has been passed on this particular date

Chinese regulators have applied to a certain degree legal transplantation – legal term meaning the incorporation of a rule or system of law from one country/region to another– into its domestic law, by including OECD international principles of privacy and data protection and adapting provisions from GDPR, such as broader scope of sensitive data. This phenomenon is observed in the Cybersecurity Law (CSL) (2017) –the first national-level law to address data privacy protection. In the summer of 2021, Data Security (DSL) and the Personal Information Protection (PIPL) were enacted. PIPL –a milestone for governing processing of personal information– was issued in the wake of enhanced scrutiny over the tech sector by the Chinese government with the most prominent case of 25 Didi-related apps that were removed from the app store for illegal use of Chinese users' information. Chinese citizens are increasingly concerned about their privacy, the data black market (for instance, theft, hijacking, fraud, and other data-based crimes), and other data protection issues in relations with the private sector. Those concerns are shared on the Chinese news and social media platforms, pressuring the CCP and lawmakers to take responsibility and action to better protect individuals' privacy.

In recent years, several enforcement campaigns show the heavy-handed approach that the Chinese authorities have taken against unlawful or unreasonable collection or misuse of personal information. As a result, a paradox exists of government accessing personal data claiming national security, while protecting consumers against private firms. This paradox demonstrates one of the great differences with the EU's and US' data governance approach. Consequently, a fragmented global data governance exists, which enhances risks for global interoperability affecting mainly users and businesses.

Understanding cyber and data sovereignty in China

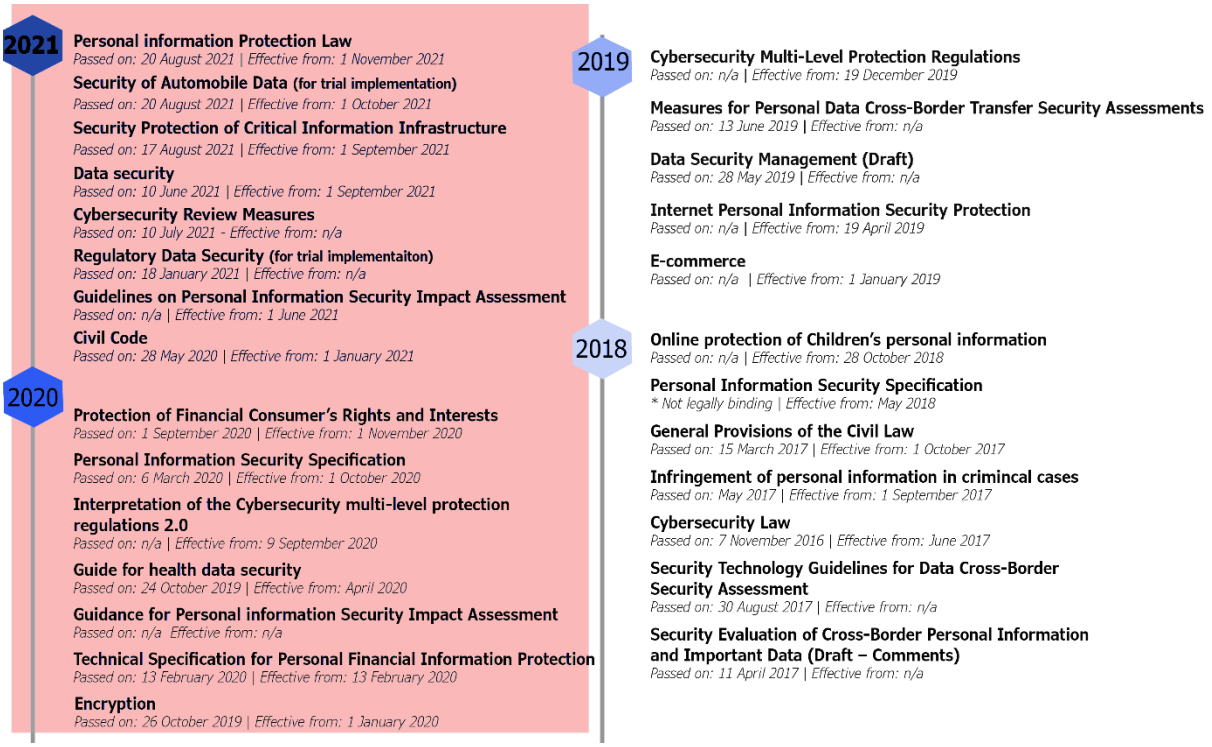
China's National Cyberspace Security Strategy (2016) highlights the relevance of national security over cybersecurity and data security. According to the definition of CAC, Internet/cyber sovereignty (网络主权, *wangluo zhuquan*) is governed by the State, who has the right to oversees its Internet and assert national jurisdiction over information and communication infrastructure, as well as resources and information and communication activities. Hence, data protection is understood within the cyber sovereignty framework and a distinction between privacy from the government and private sector.

Yet, China asserts the legitimacy of governmental control over data flows advocating for cyber sovereignty and data sovereignty. Territorial data localisation is perceived as a legal instrument to assert data sovereignty. China's data governance regime allows foreign companies to comply with its regime only within mainland China while operating differently elsewhere.

To assert data sovereignty, China's legal instruments apply to territorial data localisation (CSL Art. 37, PIPL Art. 39-38). Regulators assert the legitimacy of governmental control over data flows advocating for cyber and data sovereignty. These concepts are central to China's data governance regime and shape how China-headquartered companies and individuals engage with the outside world and vice versa.

Figure 3

Laws, regulations and national standards related to personal information protection (selected)



Conclusion and policy recommendations

An increasing debate has emerged in relation to privacy, national security concerns, and technological and economical hegemony, especially in Europe. National and supranational data regulations are constantly evolving. The US and China's regimes both present challenges to the EU data governance approach. Yet, economic and values principles, state sovereignty, and international commitments are far from being reconciled. The proliferation of regulatory forms that involve multiple stakeholders with varied types of supervisors, create divergences in the approaches of the EU, PRC, and US. This results in a fragmented global data governance that we describe as a triple regime risk.

The EU should avoid to perpetuate a fragmented global data governance that contributes to data protection interoperability problems and international trade barriers. The changing political landscape, the raise of trade-tech frictions between the US and China, and the triple data governance regime call for urgent and effective multilateral initiatives for aligning data governance approaches. The EU should reconcile individuals, private, and public sectors' interests, which, at the same time, calls for a data governance regime combining top-down and bottom-up political approach and regulation.

The EU needs to support small and medium-sized entrepreneurs' (SME) growth because fragmentated data regimes possess high risks to SMEs. The EU does not have many global tech champions, unlike the US and China. Fragmented regimes do not necessarily incur high costs and are technologically

possible for multinational firms that are able to store and process data in different jurisdictions. SMEs, instead, are unlikely to survive under such market pressure and fragmented regulatory frameworks.

Lastly, mismatches between domestic rule-creation and the positioning of a country in global data governance exist. We suggest the establishment of multidisciplinary expert working groups that are independent from political and private interests and bring together stakeholders from the US, China, and the EU. Working groups should provide indications as to the present and future constraints upon regulatory cooperation.

Read the research that informed this brief:

Dekker, B. and Okano-Heijmans, M. (2020) Dealing with China on high-tech issues: views from the US, EU and like-minded countries in a changing geopolitical landscape. *The Clingendael Institute [online], December.*

Available at: Report_Dealing_with_China_December_2020_0.pdf (clingendael.org)

Dekker, B., and Okano-Heijmans, M. (2020). Europe's digital decade? *The Clingendael Institute*, [online] 21 October.

Available at: https://www.clingendael.org/publication/europes-digital-decade

Paulo (2021). Digital Connectivity: impact on relations between EU and China, Japan, South Korea. in: Special Issue by the European-Asian Research Network on Strategies for Promoting Europe-Asia Connectivity (SPEAC), submitted for publication in *Asia Europe Journal*.

Paulo, M. and Bersick, S. (2021). China, the EU, and Digital Connectivity. In: Monograph Issue by the European-Asian Research Network on Strategies for Promoting Europe-Asia Connectivity (SPEAC), planned to be published in 2022 in *Asia Europe Journal*.

Paulo, M. and Vasquez, M. (2021). Assessing the interoperability of the Pacific Alliance's and China's data protection approaches: The Case of TikTok. Working Paper. Submitted for publication. Forthcoming.

This publication is based upon work from COST Action CA18215 - China In Europe Research Network, supported by COST (European Cooperation in Science and Technology).

COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation.
https://www.cost.eu/

https://china-in-europe.net/

Get in touch with the authors:

Mireia Paulo, A&Z Law Firm & Ruhr-Universität Bochum
mireia.paulonoguera@rub.de

Brigitte Dekker, Clingendael Institute
bdekker@clingendael.org

cost EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

Funded by the European Union

CHERN China in Europe Research Network CA18215