BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 5 • N° 17 • AUGUST 2019

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

DATA LOCALISATION: DECONSTRUCTING MYTHS AND SUGGESTING A WORKABLE MODEL FOR THE FUTURE. THE CASES OF CHINA AND THE EU

Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China

Edited by Vagelis Papakonstantinou, Brussels Privacy Hub

Data localization is highly controversial, being ultimately connected to the topic of national sovereignty in the age of the internet. Opponents believe that it constitutes a trade barrier and undermines global connectivity. Supporters point out that states need to exercise control over data as a matter of national security. It remains doubtful whether differences can ever be bridged, because each side's argumentation can be traced back to, basic, state theory: The internet only extrapolates onto modern digital circumstances old arguments about the role of states, the rights and freedoms of individuals, global cooperation and free trade. A number of popular myths further complicates understanding. Faced with differences in political and even philosophical approaches, this paper aims to dispel misunderstandings and present a workable and realistic model for data localisation exercises based on a "reasonable limitation" principle for the local storage of data.

Keywords: Data localization, data sovereignty, cross-border data flows, the principle of reasonable limitation for the local storage of data

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.

Disclaimer

Introduction

Data localization, as opposed to the cross-border flow of data, refers to the policy or rules formulated by a government to restrict digital data from leaving the country.[1] In the Internet era, data naturally flows across national boundaries and gains value due to the flow. It has become a basic consensus that data flow can lead technology flow, capital flow and talent flow.[2] In this sense the requirement of data localization seems to run counter to it. Opponents of data localization regard it not only as a trade barrier, but even as a way to undermine the global interconnectedness of the Internet and thus overturn the existing world order.

Notwithstanding the fact that disputes ultimately originate from different worldviews (globalization vs local) and even philosophical approaches (what is the role of states, what are the rights and freedoms of individuals), the term itself does little to assist understanding and offer clarity. This is not so much on account of its choice of words, but rather due to their vagueness in a digital context: What is "data"? Does it include each and every type of data? Government data? Military data? State secrets? Proprietary data created by private actors? Personal data? Sensitive personal data? In the same context, what is "local"? Are we to understand a territorial context? A jurisdictional context? An electronic access context?

Data localisation is not a policy met only in a particular place of the world or confined to a small list of countries. In fact, quite a few states have in one sense or another introduced data localization requirements. Which ones and how many is more dependent upon the level of their technological sophistication and level of digitization than on their political or legal regime.

As far as China is concerned, the requirement of localized data storage is not unprecedented. ***Administrative Regulations on Credit Investigation Industry*** promulgated in 2013 by State Council, ***Administrative Measures of Population Health Information (For Trial Implementation)*** issued in 2014 by National Health and Family Planning Commission of the People's Republic of China (NHFPC), ***Notice for Banking Financial Institutions to Get the Personal Financial Information Protection Work Well Done*** that People's Bank of China (PBOC) released in 2011 and ***Regulations on the Administration of Internet Publishing Services*** released in 2016 by State Administration of Press, Publication, Radio, Film and Television and Ministry of Industry and Information Technology etc., have put forward clear requirements for data localization.[3]

Different from the above provisions limited to specific departments or industries, ***The Cybersecurity Law*** makes general provisions on data localization in a comprehensive way due to its status as "the basic law of cyberspace",[4] which has attracted extensive attention from all walks of life at home and abroad. On August 11, 2016, the Financial Times reported that more than 40 industry organizations in the US, Japan and Europe launched "the biggest negotiation with the Chinese leadership since 2010", called on the Chinese government to revise ***The Cybersecurity Law***, "their worries focus on certain content of the Chinese new law, including forcing foreign

1 See Chander, Anupam and Uyen P. Le, 2015, "Data Nationalism", Emory Law Journal, v. 64, pp.677-739. P.680. Note: In this article, "data localized storage" and "data localization" are mixed without distinction. In addition, this article mixes the concepts of "data" and "information". It may be considered that data is the carrier of information, and information is the practical content presented by data. However, most national legislation does not strictly distinguish data from information.
2 Xi jinping: Strive to build China into a cyber power, http://news.xinhuanet.com/mrdx/2014-02/28/c_133149933.htm
3 See discussions below.
4 See article 37 of the cybersecurity law.

companies to store data in the territory of China", and "warning that the laws and regulations pose a protectionist threat to economic growth and will further isolate China from the global digital economy."[5] In addition, for two consecutive years in 2015 and 2016, by the way of surveys and interviews of member companies conducted by the US-China Business Council both found that the Chinese government's requirement for data localization was the biggest concern for US companies operating in China.[6]

The EU is in principle not directly comparable to China, because it is not a single state but a union of sovereign Member States. Most prominently for the purposes of this paper, matters of national security remain regulated by each Member State alone. It is therefore possible for any Member State to impose data localisation requirements for any data that it considers relate to its state security. Other than that, the EU has indeed tried to tackle the difficult problem of data localisation within its own fields of competence: Having distinguished between "personal" and "non-personal" data, it has introduced appropriate legal provisions for each. These provisions in principle have to deal with this issue in a twofold manner: First, at an intra-EU level, as regards flows of data among Member States. Second, at an external EU level, as regards international data transfers. In addition to that, the EU has started developing its own cybersecurity laws, that could, but at the moment do not, also deal with the issue of data localisation.

The lack of clarity met at a high, regulatory level has not left practice unaffected. Digital data today are handled by anybody, in his or her daily practices. Businesses and organisations customarily deal with large databases of digitized information. How are they to know where to store what information? Faced with technological tools that easily transcend borders, and having at all times to strike a balance between budgetary constraints and user-friendliness and usability of the technologies used while remaining within lawful boundaries, administrators, data controllers and other parties concerned are often faced with practical questions difficult to address with the legal instruments at hand.

The structure of this paper is as follows: After some definitional clarifications (in Part I), followed by the purpose and main international objections to data localization (in Part II), existing, in effect regulations and practices of data localization globally will be summarized (in Part III). Taking concerns and different opinions into account, Part Four will put forward a severity model, describing data localization as a yardstick to measure the localization practices of various countries, in order to point out that there is a spectral progressive approach to data localization measures, and the severity varies from country to country. Finally, Part Five will introduce a "reasonable limitation" principle for the local storage of data, that we believe can be employed globally. We believe that this principle provides a workable model for (mainstream) administrators, data controllers and processors, offering a balanced approach between the end and the means in terms of appropriateness and necessity. as to provide support or reference for legislation.

5 Financial Times Chinese website: "China's cybersecurity rules will hinder growth," August 11, 2016. http://www.ftchinese.com/story/001068889

6 The US-China Business Council, Technology Security and IT in China: Benchmarking and Best Practices, July 2016. For the full report, seehttps://www.uschina.org/reports/technology-security-and-it-china-benchmarking-and-best-practices

1. A brief note on terminology: Data localisation and neighboring terms

1.1. Data localisation, data sovereignty, data residency and data nationalism

There is notable lack of clarity when it comes to the notion of data localisation. First, with regard to the term itself: A number of different implementations, either theoretical or already viewable across the globe, of varying degrees of localisation requirements blur the picture of what data localisation really is. Chapter IV, analyzing a data localisation severity model, will deal with these options and with nuances that substantially affect data localisation.

A second source of confusion is created by neighboring terms. Other than data localisation, also "data sovereignty" and "data residency" are terms frequently used, sometimes interchangeably with data localisation. However, here too significant differences can be met: "Data sovereignty" refers to the powers of states over data created within their jurisdictions. It therefore is a term belonging to state theory and opening such questions as to the extent, reasoning and consequences of such a relationship.

"Data residency", on the other hand, denotes the place where data are stored. This place is an element of choice by administrators or controllers, therefore the perspective here changes from that of the state, in "data sovereignty", to that of (normally) private actors making a decision on where to store their data.

Data localisation, unlike the above terms, denotes an obligation rather than an option or a state theory. Data localisation refers to the requirement, to a larger or lesser extent, for data to be kept in a particular place.

Finally, data nationalism[7] is a political term referring in a negative manner to efforts of states to "put up barriers to the free flow of information across the globe". In this case, an "era of a global Internet" is advocated.

1.2. A typology of digital (and digitized) data

The first component of "data localisation" is equally difficult to define. "Data", in the sense of digital data can be difficult to conceptualize in a world practically composed of them. In essence, other than physical objects, whatever else humanity today produces or deals with are "data". Even with regard to physical objects, technologies such as the Internet of Things warrant that data are connected to them as well, either intrinsically or in an added-value manner.

In order to devise a typology to assist the purposes of this paper the following categories may be, broadly, foreseen:

7 See A Chandler/Le U P, "Data Nationalism", Emory Law Journal, 2014 (http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf), and also C Kuner's reflections in "Data Nationalism and its Discontents", Emory Law Journal, 2015 (http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf)

2. Purpose and main objections to data localisation

2.1. The aims and purposes of data localisation: Data security and protection of the individuals' data

This section will analyze what can be achieved by data localization, which mainly has three levels.

2.1.1. Data Security

Data security can be recognized as information security. Information security mainly pursues three modes, known as the CIA: ***Confidentiality***, refers to information not being leaked without the grantee's permission. ***Integrity***, refers to the property of information that remains unaltered during storage or transmission without authorization. ***Availability***, refers to the availability of information that can be accessed and used by authorized persons.[8] In other words, data security means to protect information or information systems from unauthorized access, use, disclosure, damage, modification, destruction and so on.[9]

2.1.2. Protection of individuals' personal data

Data protection and privacy in European law are two different concepts. Most obviously, in the Charter of Fundamental Rights of the European Union, data protection and privacy are two different rights and governed by two different articles (see table below).

Article 7 Respect Private and Family Life	Everyone is entitled to respect for their private and family life, private apartments and private correspondence.
Article 8 Personal Data Protection	Everyone has the right to protect their personal data. The processing of personal data must be conducted in a fair manner for a specific purpose, with the consent of the individual or for other legitimate reasons as provided by law. Everyone has the right to access or correct the personal data they are collecting. Compliance with the above rules should be ensured by an independent authority.

Privacy can be understood as "leave me alone", which means the right not to be disturbed in one's private life – "I alone have the right to privacy and quiet in my personal life, which others may not violate, disturb or touch".[10] It is obvious that the right of privacy is an defensive mechanism used by an individual to resist external prying into and invasion of his or her personal domain, private information, and is an internal protection for the individual's personal domain.

8 Almost any textbook on information security will introduce the three characteristics of CIA in the first chapter and regard them as the basic principles of information security. See Michael T. Goodrich and Roberto Tamassia, 2013, Introduction to Computer Security, Pearson, "Chapter 1: Introduction".

9 See also stipulated in article 10 of the *Network Safety Law*, "construction, network, or through the network to provide service, shall be in accordance with the provisions of the laws, regulations and compulsory requirements of national standards, technical measures and other necessary measures to ensure the secure and stable operation of the network, to respond effectively to the network security incidents, to prevent network illegal and criminal activities, to maintain the integrity of the network data, confidentiality, and availability." This article summarizes the security of network data as integrity, confidentiality and availability.

10 In 1890, American jurists Samuel d. Warren and Louis d. Brandis first proposed the article entitled "The Right to Privacy" published in *Harvard Law Review*.

The classical understanding of privacy rights conforms to the meaning of article 7 of Charter of Fundamental Rights of the European Union.

The right to protect personal data is based on the theory of "self-determination of personal information". The theory holds that in order to guarantee the free development of personality, individuals should be free to decide which way to realize the development of personality. The formation of personality is mainly realized in the process of communication between people and the outside world, especially between people. Therefore, individuals need to control the degree of external self-disclosure or performance, in order to maintain a reasonable interpersonal relationship between themselves and others. Therefore, individuals should be able to decide how to use personal information freely and independently.[11] That is to say, data protection rights entitles individuals to control what purpose personal data is for, what object range it is targeted at, and how it is spread and disclosed. In other words, it is "the right of an individual to control his or her personal information and decide whether or not to collect and use it, in accordance with the law."[12]

Data protection and passive defensive privacy is different, its "put itself in interpersonal interaction scenarios, so that the confidentiality of personal information and personal private domain decoupling, whether the specific content of personal information relating to the data subject personal secret, it is protected by law, because of the reasonable use and control of an individual self-expression of interest".[13] Therefore, data protection is a mechanism to manage information diffusion and disclosure, and an externally oriented control. The theoretical basis of the right to data protection stipulated in article 8 of Charter of Fundamental Rights of the European Union is to guarantee the right of "self-determination of personal information". [14] The word privacy is not used in the text of Europe's latest general data protection regulation (GDPR), also it is an example of a European distinction between privacy and data protection.

From the above discussion, it can be made clear that data protection mainly lies in "protecting the independent use of personal information and requiring others not to process personal information in a way that is against their own will. This is because the non-consensual information processing will result in a result beyond one's expectation in the society and have an unpredictable impact on one's personality development, making the result of one's personality shaping deviate from the original expectation.[15]

Professor Wang liming used the concept of personal information right to express the basic tenor of data protection: "The right of personal information mainly refers to the control and independent decision of personal information. The content of personal information right includes the right to know about the collection and use of personal information, and the right to decide whether to use or authorize others to use personal information. Individuals should have some control over personal information that can and must be made public. For example, the right holder has the

11 Xie Yuanyang, "The Value of Personal Information from the Perspective of Information Theory -- Review the Privacy Protection Mode", *Tsinghua law*, no.3, 2015, pp. 102-103.
12 Wang Liming, "On The Legal Protection of Personal Information Right -- Dividing the Right to Personal Information into Two Parts", *Modern Law,* 2013, 4 (64). See also Wang Liming: the redefinition of the concept of privacy, *The Jurist,* 2012 (1).
13 Liao Yuyi: "Definition of the Scope of Personal Information Protection in China -- on the Distinction between Personal Information and Personal Privacy", *Social Science Research*, no.2, 2016, page 72.
14 Orla Lynskey, 2015, The Foundations of EU Data Protection Law, Oxford University Press, P91-106.
15 Xie Yuanyang, "The Value of Personal Information from The Perspective of Information Theory -- And The Review Of Privacy Protection Mode", *Tsinghua law,* 2015, 3 (102-103).

right to know to what extent the information is disclosed, to whom it is disclosed, and for what purposes the information will be used by others.[16]

Thus, the conceptual distinction between data security and data protection should be obvious. First of all, there is certainly no data protection if there is no data security, because the information system is breached, the data is leaked, then the authorization of data protection requirements and control mechanism of proliferation is out of the question. Secondly, it should be noted that even if data security is achieved, data protection is not necessarily achieved. For example, data is stored safely in the information system of an organization, but the organization does not process data according to the scope authorized by the data subject, which violates the individual's data rights.

This is why the provisions on data security are independent but not too long in individual data protection legislation of various countries. Taking GDPR as an example, the focus of legislation is to stipulate the basic principles of personal data processing,[17] the rights of data subjects,[18] and the duty allocation of data controllers and processors so on. Data security is only one of the many obligations of data controllers and processors, and it's more important obligation is to provide various mechanisms in data collection, storage, use, sharing, disclosure, cross-border transmission and other links, so that data subjects can exercise their "right of information self-determination". For example, the controversial right to be forgotten is a major innovation of GDPR. Apparently, the right to be forgotten has nothing to do with data security, but entitles individuals to delete their personal data in specific circumstances.

2.1.3. Which data for which data localisation? The state's viewpoint

Personal data protection protects (almost exclusively) the data of individuals. As mentioned above, however, there are many other categories of "data" that may fall under data localisation requirements. Three relevant examples, that demonstrate the difficulty to distinguish, will be discussed here:

According to Alibaba's quarterly results at the end of September 2016 released on 2 November 2016, the number of active buyers on taobao's Chinese platform reached 439 million. [19] According to taobao's privacy policy, taobao buyers are required to submit at least the following information: name, gender, date of birth, id number, passport surname, passport name, passport number, phone number, email address, etc.[20] Combined with the above information, it can be inferred that Alibaba control at least the basic personal information of 400 million Chinese citizens. And with the help of the buyer to pay, receive goods and other scenes, its grasp of the authenticity of the data and even far beyond the government. The basic information of an individual citizen

16 Wang Liming: "On The Legal Protection of Personal Information Right -- Dividing The Right to Personal Information and the Right to Privacy into Centres", *Modern Law*, 2013, 4 (67).

17 See chapter II of the GDPR The basic principles include "legality, fairness and transparency", "purpose constraint", "data minimization", "accuracy", "storage restriction", "security" and "accountability". For full text of GDPR, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

18 See chapter III of GDPR. The rights mainly include the right to know, the right to query, the right to correct errors, the right to delete (forgotten), the right to limit data processing, the right to carry data, the right to oppose data processing, the right not to significantly affect the individual, the right to make decisions in an automated way.

19 Alibaba group: "alibaba group announced the quarter results end of September 2016 ", http://www.alibabagroup.com/cn/news/article? News = p161102

20 Taobao: Legal Statement. https://www.taobao.com/go/chn/tb-fp/2014/law.php?spm=a21bo.50862.1997523009.38.26IY3m

undoubtedly belongs to the personal information that should be protected. And a private enterprise has gathered such a large amount of personal information of citizens, whose significance obviously goes beyond the protection of individual rights and interests.

The second example is that Kaspersky, a well-known Russian network security manufacturer, publicly protested that Microsoft squeezed the living space of third-party anti-virus software in the win10 operating system in November 2016.[21] On the face of it, this is about business competition. But more than that, it's a matter of national security. President Xi jinping has pointed out that the key to maintaining cyber security lies in "all-time and all-directional perception of cyber security situation".[22] Therefore, without the security big data gathered by network security information such as network attack, threat source and malicious address, it is impossible to "know yourself and your enemy". Microsoft's exclusion of other antivirus software from its ecosystem has objectively resulted in a monopoly on the security big data generated around its platform.

The third example concerns the housing vacancy rate. According to the industry, the vacancy rate mainly refers to the vacancy rate of the unused housing divided by the total housing in the whole society at the statistical moment. Once "The vacancy rate exceeds 5 to 10 percent, there will be a big problem in the real estate market: a serious oversupply of houses, rents and house prices will start to fall." Moreover, "the housing vacancy rate reflects the waste of social resources. The high vacancy rate reflects the fact that the investment property of housing has been infinitely amplified and exaggerated in recent years, while the residential character of housing has been diluted and weakened, which reflects the reality of the serious polarization between the rich and the poor in Chinese society".[23] In China, the housing price is one of the things that the government and people are most concerned nowadays. Therefore, especially when the government introduces regulatory measures, the vacancy rate is likely to become a "statistical report with great influence on macroeconomic regulatory policies and measures", or "statistical data and reports reflecting major economic and social issues", which belongs to the category of state secrets. [24] This also explains why some local statistical departments have conducted surveys on the vacancy situation of local houses but never release the results.[25] In the past, scholars or private forces could only calculate the vacancy rate through "counting black lights" or household sampling survey. Now, it is not difficult to get an accurate vacancy rate in a certain region or even the whole country by combining massive express orders, water and electricity operation and other data.

All three examples show the growing significance of big data for national development, governance and security. First of all, the population information possessed by Alibaba is comparable to the national population basic information database of the public security organ in terms of

21 Kevin Townsend, "Kaspersky Lab Accuses Microsoft of Aggressive Attitude Towards Endpoint Security Firms With Windows 10", November 15, 2016, http://www.securityweek.com/security-firms-allege-microsoft-anti-competitive

22 Xi Jinping, "speech at the symposium on cybersecurity and informatization," April 19, 2016, http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm

23 Meng bin, Cao Jianhai, Jiang wei, Chen guoqiang: "why vacancy rate becomes a secret", *China fortune*, 2010, 10 (P90).

24 See "notice of the national bureau of statistics on the interpretation of statistical work items in the regulations on the printing and distribution of state secrets and the specific scope of their categories in economic work", http://www.stats-fj.gov.cn/xxgk/fgwj/gfxwj/201211/t20121114_35768.htm

25 Netease Curated, "housing vacancy rates: always debated, never settled," http://gz.house.163.com/special/gz_kongzhilv/

size and granularity, and even more accurate. For the country, once the basic population data is leaked, it is likely to cause serious harm to national security.[26]
Secondly, in addition to data security, the state shall have a certain degree of domination due to the fundamental and strategic role of certain big data for the country. For example, if the big data of China's population gathered by Alibaba is not classified as a secret-related system, the state shall at least have the right to request that it shall not be shared or traded with other countries, and shall not provide it to overseas organizations or individuals. For the second example, given the large number of users of Microsoft operating system in China, the country should have the right to require Microsoft not to monopolize, or even to share with the competent authorities' win10 platform produced in China's network security big data. This is not only because the security big data generated by a large number of users is crucial to the maintenance of national network security. Another reason is that if the big data of security can be used to improve the security level, vice versa, the security of big data can certainly be easily used by malicious elements to analyze the vulnerabilities of the system so as to find the entry point of attack.

In the third example, Taobao, SF and other enterprises obviously have a large amount of express order data. At present, Alipay, WeChat and other applications have integrated the payment function of life, which is favored by more and more families. These two types of data are not state secrets. But the combination of the two makes it easy to synthesize and come up with highly protected state secrets. In fact, the development of big data has led to the blurring of the boundary between state secrets and non-state secrets. For "data that may have adverse effects on national security and public interest after analysis alone or in combination with other information", this paper calls it sensitive data. Obviously, the scope of sensitive data is much larger than the range of "state secrets" identified in practice. Although it is not a realistic option to include all sensitive data in the "state secrets", such a compulsory mechanism directly controlled by public power, there is indeed a strong objective needed to prevent such sensitive data from malicious use of big data by hostile countries or forces, such as malicious release of relevant information at critical time nodes that will harm China's economic security.

2.2. Objections

Many objections have been raised against data localisation practices. First, in terms of economy, many commentators have pointed out that the data localization is out of step with the current high-speed flow of information, capital, technology and talents in the global economy, which will seriously affect efficiency and slow down the industrial development and technological progress. A series of research papers published by the European Centre for International Political Economy (ECIPE) suggest that the adoption of data localization measures will cause losses to a country's real GDP, for example, such localization will cause 0.48% of GDP losses to the EU, 0.25% to India, and 0.55% to China. [27] After a special topic research on the measures of data localization carried

26 Turkey has a population of 80 million. In April 2016, the personal information of nearly 50 million Turkish citizens held by the Turkish national police was leaked and sold on the black market. The data contained personal and family information of former and current Turkish state leaders. See Doug Olenick, "50 million exposed in Turkish data breach", April 04, 2016, https://www.scmagazine.com/50-million-exposed-in-turkish-data-breach/article/528739/

27 Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, 2016, Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization, Global Commission on Internet Governance Paper Series, P10. https://www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-data-and-data-localization. For other reports, see Bauer, Matthias et al, 2013, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce." https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf Bauer, Matthias et al, 2014, "The Costs of Data Localization: Friendly Fire on Economic Recovery." ECIPE Occasion Paper no. 3/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

out by Russia, some scholars have concluded that the GDP of Russia will decrease by 0.27% [28]due to such measures. Other commentators hold that countries which adopt the regulations of data localization aim to support domestic industries and enterprises, and improve domestic employment by cracking down on the competitive advantages of US IT giants.[29] Such action actually constitutes a serious digital trade barrier. [30]

Second, in terms of internet technology, some commentators have pointed out that the mandatory regulations of storing data within the territory violates the original intention of internet design, which will further undermine the open and interoperable Internet architecture. ***One Internet***, the final report published by the Global Commission on Internet Governance in June, 2016, indicates that the data transmission on the Internet follows the principle of efficiency and does not consider border factors. [31] Regional restrictions imposed on such transmission will "shake the stability of the Internet infrastructure".[32] Other commentators hold that the requirement of data localization essentially conflicts with the logic of the information technology development, such as cloud computing, big data and the Internet of Things (IoT).[33] Illustrated by the big data, if the data localization is mandatory, it implies that the data cannot move from the local area and all overseas data must be transferred to the local area for combination. If other countries or regions also have similar clauses of data localization, the sum of data that can be collected together will decrease. As a result, the influence that the big data could have will also be decreased.[34]

Third, in terms of Internet governance and even world order, some commentators have pointed out that the mandatory regulations of storing data within the territory implies that such country forcibly brings the data under its control of sovereignty regardless of technical reality and world trend. BRICS countries such as China and Russia behaves rather actively. The attempt by these countries to build an Internet with BRICS characteristics will eventually lead to the division of the Internet, namely, Balkanization.[35] There are still many commentators who further regard the data localization as one of the specific form of internet sovereignty, and regard the conflict between internet sovereignty and global Internet governance, represented by the multi-stakeholder model, as one of the epitomes of Sino-Russian and US-Western contention for the leadership of the world order.[36]

28 Lee-Makiyama, Hosuk, 2015, "Data localization requirement in Russia." http://www.ecipe.org/blog/data-localisation-russia/

29 See Lee-Makiyama, Hosuk, 2013, "European leaders show leave data flows open." http://www.euractiv.com/infosociety/european-leaders-leave-data-flow-analysis-530785 Aaronson, Susan and Maxim, Rob, 2013, "Data Protection and Digital Trade in the Wake of NSA Revelations." http://elliott.gwu.edu/sites/elliott.gwu.edu/files/downloads/research/aaronsonData%20Protection%20and%20Digital%20Trade%20in%20the%20Wake%20of%20the%20NSA%20Revelations.pdf

30 AmCham China, 2015, "Protecting Data Flows in the US-China Bilateral Investment Treaty." http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization US Chamber of Commerce: "Safeguard Cross-border data flows.", 19 May 2015, https://www.uschamber.com/issue-brief/safeguard-cross-border-data-flows Office of the United States Trade Representative, 2015, "Trans-Pacific Partnership: Summary of US Objectives." https://ustr.gov/tpp/Summary-of-US-objectives

31 Global Commission on Internet Governance: One Internet, June 21, 2016, P36 https://www.ourinternet.org/report

32 Id P55.

33 Anupam Chander and Uyen P. Le, 2014, Breaking the Web: Data Localization vs. the Global Internet, UC Davis Legal Studies Research Paper No. 378, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858

34 Richard Bennett, "Surge in data localization laws spells trouble for Internet users", May 10, 2016, http://www.techpolicydaily.com/internet/surge-in-data-localization-laws-spells-trouble-for-internet-users/

35 Dana Polatin-Reuben and Joss Wright, 2014, An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet, 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2014), https://www.usenix.org/node/185057

36 Dana Polatin-Reuben and Joss Wright, 2014, An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet, 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2014), https://www.usenix.org/node/185057

3. Decomposing the data localisation myth: Data localisation implementations across the globe

When engaging in a data localisation debate it is important to keep in mind the two critical questions emanating from the term's constituting parts: Which "data"? How local?

Referring to the typology of Part I, there normally is little discussion that state data falling under the national security category need to be stored locally. Confidential government documents, military data and other restricted state documents will normally need to apply strict data localisation policies. Indeed, this is the case even in countries famously against data localisation measures (see the map in subchapter 1): For example, the U.S. department of defense requires its cloud service providers to store DoD data locally.[37]

Consequently, the "data" most usually under discussion to be localised or not refers the data generated, stored and processed by private subjects including individuals, enterprises, communities and other non-public organizations and institutions.

Even in this case, however, not all private data should be placed under the same test conditions: For example, cybersecurity legislation across the globe introduces the term of "critical infrastructures". This term is meant to also cover private organisations. Should they also apply data localisation practices in their data processing?

Similar questions could be raised with other categories in the data typology above: Should PSI and other public-sector generated data freely cross borders? Why should birth certificates, tax statements, census data, weather reports, marine data, or (non-military) maps be stored outside national borders? Should the same rules apply to each one of the above categories?
Finally, an important and extensive data category, that however existing literature almost exclusively uses as its term of reference when discussing data localisation, refers to private data generated by natural persons: emails, social media profiles, use patterns of online applications, any and all digital traces created by an individual online.

3.1. Data localisation: A little discussed global trend?

According to statistics, at present, more than 60 countries in the world have made regulations on data localization,[38] as shown in the following figure. These countries are spread across all continents, including developed countries and regions such as Canada, Australia and the European Union, as well as developing countries [39]such as Russia, Nigeria and India. The darker the color in the figure,[40] the more stringent the requirements for data localization.[41]

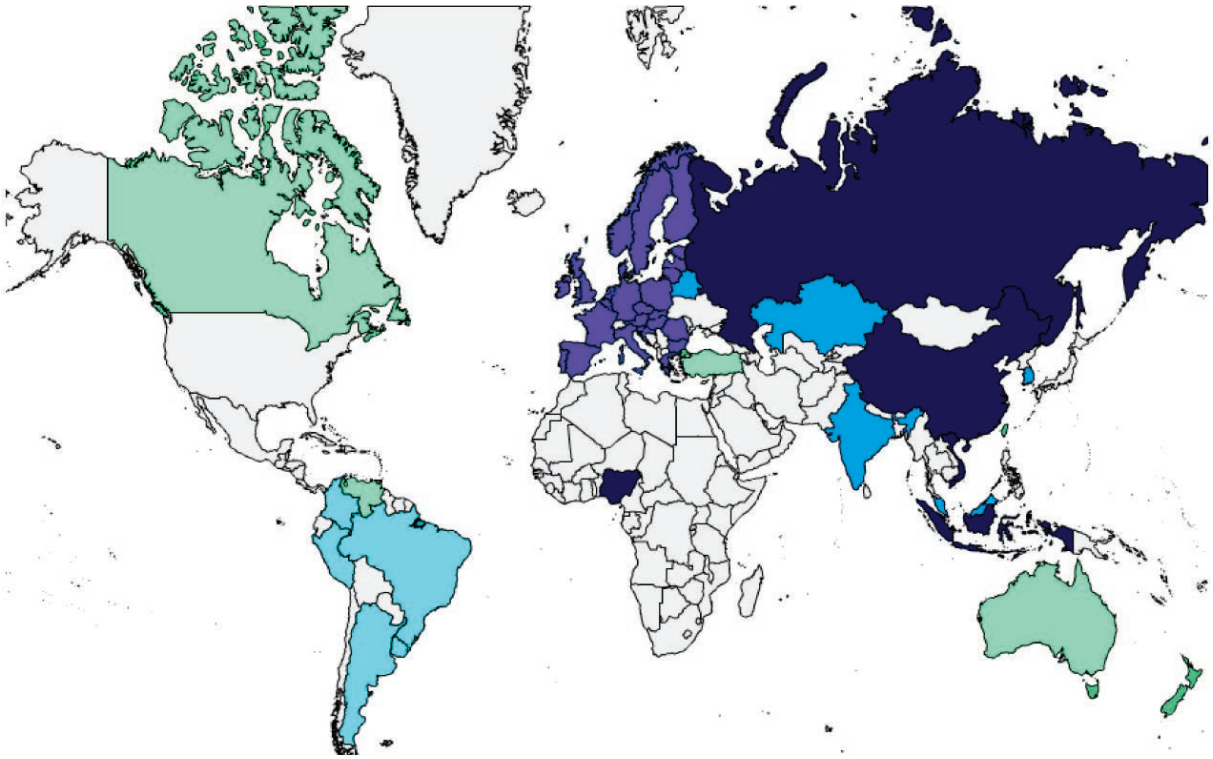
37 See DoD Interim Rule on Network Penetration Reporting and Contracting for Cloud Services.https://www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for

38 Matthias Bauer, Martina F. Ferracane, and Erik van der Marel. Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization, Global Commission on Internet Governance Paper Series. 2016. https://www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-data-and-data-localization

39 The following paragraphs will specify the data localization measures implemented by major countries.

40 According to the report from Albright Stonebridge Group, countries in light grey refer to those countries that have not been found to have regulations on data localization.

41 The report from Albright Stonebridge Group evaluates the stringency of regulations on data localization from a subject-level. In the third part, this paper will propose a model to objectively describe the severity of data localization.

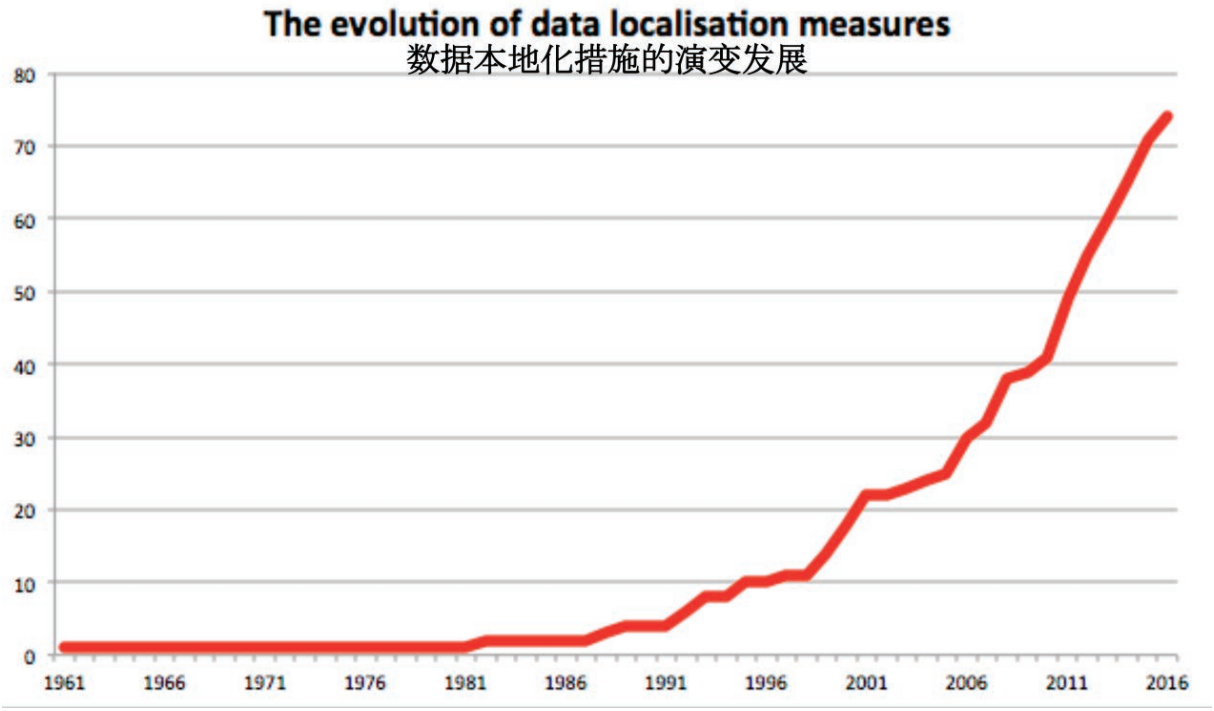


From Albright Stonebridge Group, Data Localization: A Challenge to Global Commerce and the Free Flow of Information, Sep. 2015, P5. [42]

Most of the existing data localization regulations are drafted after 2000.[43] An interesting point can be found from the following figure:[44] the rise of data localization has just coincided with the development of information technology represented by the Internet. In the era of personal desktop computer, data is stored directly on the hard disk of the computer. In the early days of the development of network technology, multiple desktop terminals in an organization were connected to only one server when the data were stored on its own server. In these two stages, the data possessor can control the data well in terms of the flow direction, storage location, access, processing etc., with the most complete control over the data.

As the cloud computing becomes popular, the data possessor's ability of control over data has been weakened. Generally, large cloud service providers have established data center in various countries and regions; an organization rents cloud service, despite of the control over the access and processing of the data, but it usually cannot control such data and be informed of the physical storage location of such data.[45] Compared with the first two stages, there is a middleman – cloud service provider, between data possessor and the data. If a data possessor wishes to obtain the control over the data, it depends on whether such "middle man" faithfully fulfills its obligations as an agent.

42 http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.
43 Martina Francesca Ferracane, How data localization wipes out the security of your data, June 2016, http://www.securityeurope.info/how-data-localisation-wipes-out-the-security-of-your-data/
44 The ordinate of this figure indicates the number of countries which take measures of data localization.
45 See the introduction to cloud computing service mode in the Information security technology—Security guide of cloud computing services (GB/T 31167-2014) Section 4.2.



From Martina Francesca Ferracane, Data Localization Trends, European Centre for International Political Economy, Presentation in Beijing, 19 JULY 2016[46]

The development of big data technology has greatly enhanced the demand of data control by data possessors on another level. Once a massive number of data is disclosed to the outside world, whether it is actively shared or passively leaked due to the breach of the information system, it may be used maliciously, for example, hostile forces will combine massive data with other data sets and conduct data mining with various algorithms, in order to analyze and master information that can threaten national security.

It is recognized that, on the one hand, the ability of data possessor to control data is weakening and the number of intermediate links is increasing; on the other hand, the demand for strengthening data control is increasing. Therefore, to a certain extent, the data localization indicates a response of data possessor to the above dilemma.[47]

3.2. China's Current Regulations and Legislative Proposals

In China, the major effective provisions of data localization are found in the laws and regulations of finance, sanitation and healthcare, and transportation (see the table below). Currently, another legislative bill of data localization in finance sector is the ***Regulatory Provisions on the Information Technology of Insurance Organizations (draft for comments)*** (the "Regulatory Provisions"), issued by China Insurance Regulatory Commission (CIRC) in October, 2015. Article 31 of the ***Regulatory Provisions*** stipulates that "if the data is generated from the place within the territory of the People's Republic of China, the physical location of the data center shall be located within the territory". Article 58 also stipulates that the data, contained in the information system of

46 Internal discussion, available upon request.
47 Wang, Yue. Analysis on the Justification of Cyber Data Localization Legislation. Journal of Xi'an Jiaotong University (Social Sciences) Vol. 36. 2016.

foreign-invested insurance organizations, transferring across the border of PRC China shall be subject to the related laws and regulations of PRC China.[48]

Laws and Regulations	Specific Clauses
Administrative Regulations on Credit Investigation Industry promulgated by the State Council in 2013.[1]	Article 24 Sorting, keeping and processing of information collected in China by credit investigation organizations shall be carried out in China.
Administrative Regulations on Maps promulgated by the State Council in 2015.[2]	Article 34 Entities engaging in internet map services shall set their servers which stores map data within the territory of the People's Republic of China, and shall establish the management system as well as protection measures for the data security of internet maps.
Measures for the Administration of Population Health Information (for Trial Implementation) issued by the National Health and Family Planning Commission.[3]	Article 10 The population health information shall not be stored on servers abroad, or hosted and leased servers abroad,
Notice of the People's Bank of China for Banking Financial Institutions to Get the Personal Financial Information Protection Work Well Done issued by the People's Bank of China in 2011.[4]	VI. The personal financial information collected inside the territory of China shall be stored, processed and analyzed also inside the territory of China. Unless otherwise prescribed by any law or regulation or the People's Bank of China, the banking financial institution shall not provide any domestic personal financial information to an overseas party.
Regulations on the Administration of Internet Publishing Services promulgated by the State Administration of Press, Publication, Radio, Film and Television, and Ministry of Industry and Information Technology in 2016.[5]	Article 8 To engage in internet publishing services, a book, newspaper, periodical, audiovisual or electronic publisher shall meet the following conditions: (3) Having the technologies and equipment necessary for internet publishing services, and the relevant servers and storage devices must be located within the territory of the People's Republic of China.
Guidelines on Acceptance Inspection for Commencement of Business of Insurance Companies issued by the China Insurance Regulatory Commission in 2011.[6]	3. Standards for acceptance inspection for commencement of business (9) Computerization shall comply with the requirements of the CIRC. Important data such as business data, financial data, etc shall be stored in China, the company shall possess independent data storage equipment and implement the corresponding security protection and off-site backup measures.
Provisional Measures for Administration of E-Hailing Services issued by the Ministry of Transport, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Commerce, State Administration for Industry and Commerce, and General Administration of Quality Supervision, Inspection and Quarantine in 2016.[7]	Article 27 An E-hailing platform company shall comply with applicable requirements of the State for network and information security, and the personal information gathered and the business data generated shall be stored and used in mainland China and be kept for at least 2 years. Unless otherwise required by the laws and regulations, the above information and data shall not be disclosed.

In the telecommunications industry, the foreign companies operated in China are required to obtain an Internet Content Provider (ICP) filing or license in practice by the Ministry of Industry and Information Technology (MIIT) based on the feedbacks from these companies. Such regulation actually constitutes the requirement of data localization.

48 Drafted for comments for the Regulatory Provisions on the Information Technology of Insurance Organizations. http://www.circ.gov.cn/web/site0/tab5168/info3975814.htm.

Recently, the regulation of great concern is that of ***Cybersecurity Law*** on data localization. Article 37 stipulates that "The operator of a critical information infrastructure shall store within the territory of the People's Republic of China personal information and important data collected and generated during its operation within the territory of the People's Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail." This is the first time that China has made unified regulations on data localization across industries.

3.3. Data localisation in the EU

4. A severity model for data localisation practices

From the above sections, it can be seen that, on the one hand, data localization seems to be favored by more and more countries with the progress of information technology. On the other hand, international public opinion and a large amount of academic research strongly oppose localization measures.

How to bridge the gap between behavior and cognition in reality? This paper proposes the following Suggestions: **firstly**, both scholars and policy makers should see that the localization measures for data are a spectral existence, and the localization measures at both ends are different in severity; With this awareness, not only can scholars avoid gross generalizations in their studies, but policymakers can choose their policy tools more accurately and precisely, and both sides can truly focus their discussions.

Secondly, it's necessary to carefully explore what objectives data localization can achieve, which is particularly important in terms of the relationship between ends and means. End is the basis of judging the appropriateness and necessity of means. Once the purpose is determined, data localization measures with different severity can be selected as the means to achieve the purpose.

In other words, through this paper the author hopes to discuss the means (data localization measures severity), purpose (the goal of data localization measures to achieve), as well as the appropriateness and necessity of connection between purpose and means, setting a reasonable evaluation standard for data localization, and checking localization measures with the standard in reality, and finally realizing data localization governance according to the law by setting a reasonable limit for it, achieving a balance between government regulation and freedom of information when multiple values collide. This is accomplished through introduction of the "reasonable limitation" principle for the local storage of data in Part V of this paper.

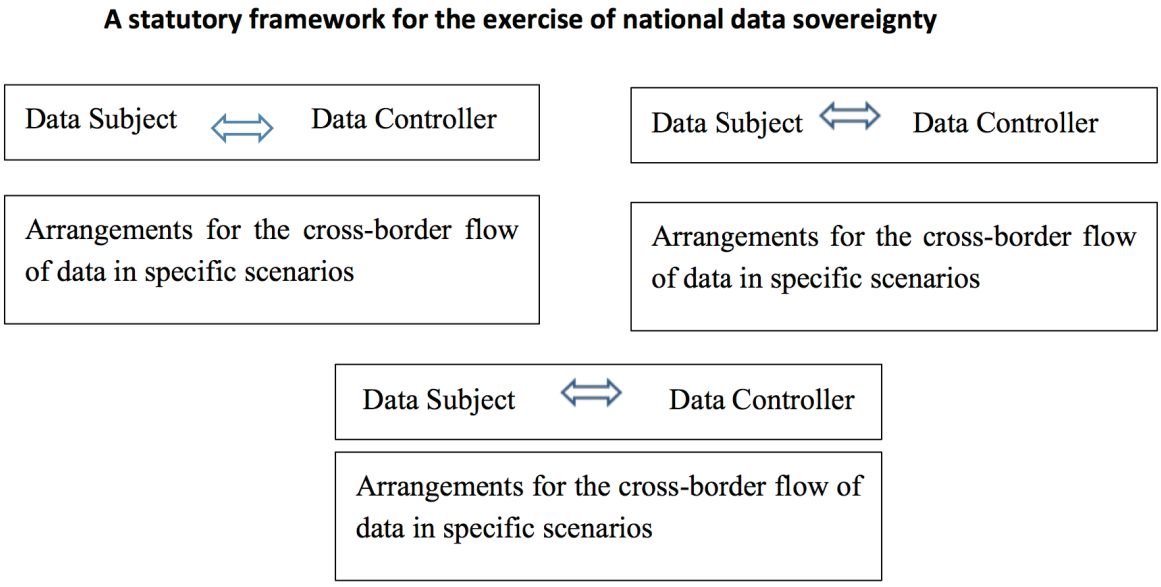
At present, most existing literatures fail to accurately describe the different severity levels of data localization.

In this paper, four dimensions are abstracted from the existing measures of various countries as indicators to construct a severity model: Implementation bodies of data localization, thoroughness of localization, data coverage of localization and exemption conditions of localization. The reason why these four metrics are abstracted in the first place is that, any localization measure must include these four dimensions logically. Different countries make different choices within these four dimensions, which constitute data localization measures with different degrees of severity.

4.1. Implementation bodies of data localisation

According to the scholar Cao lei, there are two types of body entitled to data rights -- state and citizen. States own data sovereignty, so they can "independently manage and utilize their own data". However, the subject of "data rights" is citizens, and it is the right to use data formed by corresponding citizens' data collection obligations, and the use of data is established under the sovereignty of data. Only under the statutory framework of data sovereignty can citizens exercise their data rights freely."

Now the above analytical framework is slightly modified: **At the macro level**, countries define the scope of data under their jurisdiction according to their sovereignty and set up a legal framework for data management and utilization. For example, a country enacts laws on the protection of personal information, in which the rights and obligations of data subjects (i.e. ordinary individuals), data controllers (i.e. organizations, institutions and individuals that collect, use and disclose personal information) and other relevant parties are set respectively. **At the micro level**, data subjects, data controllers and other relevant parties interact and negotiate under the statutory framework set by the state according to their respective rights and obligations granted by the state, and form specific data processing arrangements in different scenarios. Focus on the data localization in specific scenarios, whether the data is stored locally or transmitted abroad is decided by the data subject, data controller and other relevant parties through independent consultation without the direct intervention of the state. As shown in the figure below.



A statutory framework for the exercise of national data sovereignty

For example, article 17 (3) of South Korea's *Personal Information Protection Act* which came into effect in 2011 stipulates that "The consent of the data subject shall be obtained before the transmission of Personal Information to a third party outside The country".[49] In this case, the way of exercising data sovereignty by South Korea through is making a "personal information protection act"; as for whether the data is stored locally, the basic attitude of the sovereign state of South Korea is: The flow of data abroad should not be treated the same as other data processing. Therefore, the data controller shall separately inform the data subject before transferring data abroad. However, whether the data can only be retained in South Korea should be decided by the data subject. Thus, the "personal information protection law" gives data subjects the right to independently control whether their personal information flows abroad, and the data controller should follow the expression of the meaning of the data subject.

In other words, in terms of data localization, South Korea exercises its data sovereignty by taking the cross-border flow of data as a separate risk point, respecting the willingness expressed by the data subject at the same time, and giving the data subject a dominant position over the data controller in the form of individual rights. Similarly, the ministry of communications technology of India issued the "information technology act" on privacy implementation details in 2011. The rules stipulate that personal information can be transmitted abroad with the consent of the data subject. [50]

Similarly, the system design of the General Data Protection Regulation (GDPR) on the cross-border flow of personal data also reflects the feature that data sovereignty does not directly intervene in specific data processing arrangements. Based on the provisions of chapter 5, on "transmission of personal data to a third country or international organization", the following conclusions can be drawn: the basic principle and premise made by the EU, a data sovereign subject, on the cross-border flow of data is that the data receiver outside the EU should provide the same level of data protection as the GDPR. There are two ways to implement the above principles and premises: First, the European Commission determines whether legislation and data protection systems in third countries can provide the same level of data protection as GDPR. Second, if the commission has not yet made the above determination, data recipients outside the EU can also take the initiative to adopt appropriate protection measures, such as Binding Corporate Rules, to ensure that the same data protection level as GDPR is provided outside the EU.[51] In the second case, data sovereignty is not directly involved the data transfer in a specific scenarios.

Similarly, the Guidelines for Processing Personal Data Across Borders of Canada state that data importers and exporters should be held responsible for the security of data in cross-border circulation and ensure that personal data transmitted to third parties overseas are adequately protected. To be specific, the data exporter shall, by contract or other means,: 1) prevent unauthorized use or disclosure of data by a third party in the process of data processing; 2) confirm that the

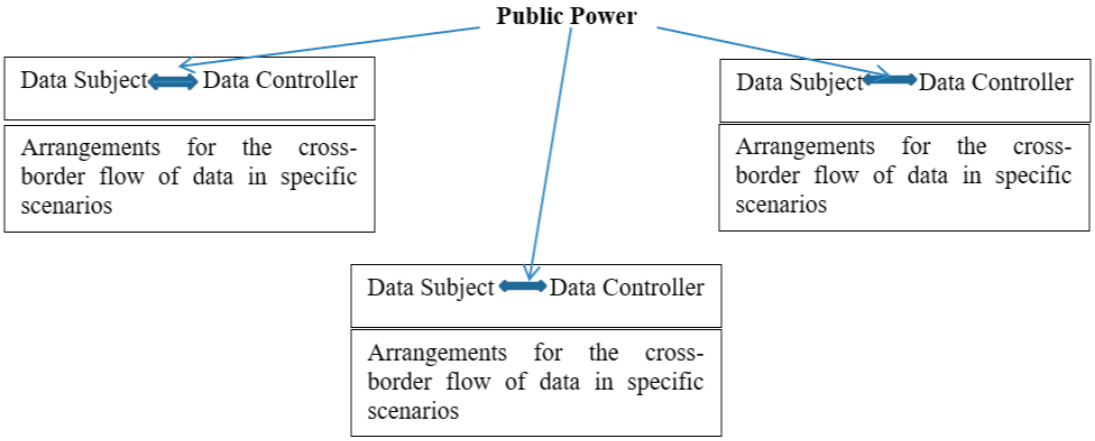
49 South Korea's *Personal Information Protection Law* in English, see: http://www.koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf

50 Chander, Anupam and Uyen P. Le, 2015, "Data Nationalism", Emory Law Journal, v. 64, pp.677-739. P.694.

51 See the full text of the *EU's General Data Protection Regulation*, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

third party has a sound data protection policy or process; 3) regularly audit the security of personal data processed or stored by a third party.[52] In other words, Canada imposes the obligation to ensure the security of data outside the country through legislation, which reflects the basic attitude of the country towards the cross-border flow of data.

While the above cases can be classified as data localisation requirements, when exercising data sovereignty, the state can break through the above macro and micro boundaries and directly intervene in the data processing arrangements independently formed by the data subject, data controller and other relevant parties as the subject of public power. As shown in the figure below.



For example, Australia's Personally Controlled Electronic Health Records Act 2012, which took effect in 2012, stipulates in article 77 that Health Records involving personal information can only be retained in Australia, otherwise they will be punished.[53] Different from the above-mentioned "backstage" of South Korea, Australia, this sovereign country directly "goes to the front desk" and forms a tri-party relationship with the data subject and data controller in the specific data processing arrangement, forcing the data to be retained in territory.

For another example, article 21 of the Personal Data Protection Law, which came into effect in Taiwan in 2012, stipulates that the competent authority should restrict "the international transmission of personal data by non-public agencies in one of the following situations": "I Involving major national interest. II There are special provisions in international treaties or agreements. III Incomplete laws and regulations of the receiving country on the protection of personal data, which may harm the rights and interests of the parties concerned. IV Circumvention of this law by means of the transmission of personal data to a third country (region)."[54] It can be seen that in the above four situations, the public authority in Taiwan will directly intervene in the arrangement of data cross-border flow in specific scenarios. [55]

52 See the full text of *Canada's Guide of Cross-border Processing of Personal Data*,https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

53 Full text of Australia's *Personally Controlled Electronic Health Records Act*, see: https://www.legislation.gov.au/Details/C2012A00063

54 For the full text of the *Personal Data Protection Law* of Taiwan, see http://www.6law.idv.tw/6law/law/%E5%80%8B%E4%BA%BA%E8%B3%87%E6%96%99%E4%BF%9D%E8%AD%B7%E6%B3%95.htm

55 Article 22 of the personal Data Protection Act in Taiwan also stipulates: ", municipal or county (city) government to carry out data file security maintenance, business termination data processing method, international transport restrictions or other routine business inspection and necessary or concern is in violation of the provisions of this law, may inspect in performing duties to carry documents, get inside to check, and may order the relevant staff to provide necessary instructions, cooperate measures or prove information "; "The competent authority or the government of a municipality directly under the central government or a county (city) may withhold or duplicate personal data or files that may be seized or may be used as evidence during the examination referred to in the preceding paragraph. The owner, holder or custodian may be required to present or deliver the thing to be withheld or copied; Those who refuse to present, deliver, or resist detention or reproduction without

As mentioned above, there are two patterns in terms of the implementation subject for data localization. The first pattern, which is called "**sovereign internalized in private rights**" in this paper indicates that the states will not intervene directly but fade in background. The will of data sovereignty enables the data subjects, data controllers and other relevant parties at the front desk by the way of "dance with the chain" to independently achieve the cross-border data flow arrangement in specific scenes by explicitly stating the basic principles of data flow and defining the rights and obligations of the behavior subjects. In this mode, as the will of data sovereignty has been reflected, public authority often only needs to verify the cross-border data flow arrangement independently reached by private subjects in the event and after the event according to the established basic principles of data flow.

In the second mode, which is called "**direct participation of sovereignty**" in this paper, national data sovereignty directly intervenes in the form of public power, and takes the data subject, data controller and other relevant parties as the behavior subject of the cross-border flow arrangement of data in specific scenarios. At this time, public power, as the main spokesman of national data sovereignty, often needs to give approval or evaluation in advance according to the cross-border flow of data in specific scenarios, make individual discretion, and deeply participate in the final cross-border flow arrangement.

It can be seen that in the two models, data localisation is not absent. However, the way to achieve its will is different, the depth and time point of intervention are different, and the discretion space of public power is also different.

4.2. Data Localization Thoroughness

To be specific, the degree of localization thoroughness includes the following three levels: **first**, only copies of data are required to be stored locally, within the territory of a specific state, while data can be stored, processed and accessed abroad. For example, the Indonesian ministry of communications requested that organizational bodies should establish data disaster preparedness centers in the country.[56] For another example, Russian federal law no. 242-fz, which took effect in September 2015, requires that "the collection, recording, collation, accumulation, storage, update, modification and retrieval of personal data of Russian citizens shall all use servers in the Russian federation".[57] Literally, Russian personal data was required to be stored, processed and accessed within its territory, but before the law took effect, the Russian department of communications and mass media issued a non-binding clarification for the law in August 2015. According to the Russian ministry of communications and mass media's interpretation of federal law no. 242-fz, personal data can be freely transmitted abroad as long as the organization has a copy of the data in Russia (even in paper form).[58] In China, the provisions on the data localization in the

good cause may be compelled to do so by means that will cause the least damage to the rights and interests of the non-public organ. Therefore, in Taiwan, the extent to which public power can intervene in the cross-border transmission of specific data can be seen.

56 Chander, Anupam and Uyen P. Le, 2015, "Data Nationalism", Emory Law Journal, v. 64, pp.677-739. P.699.

57 Full text of Russia number of 242 - FZ federal law in English, see https://pd.rkn.gov.ru/authority/p146/p191/

58 A summary of a non-binding clarification issued by the Russian ministry of communications and mass media in response to federal law 242-fz, see http://www.law360.com/articles/698895/3-things-to-know-about-russia-s-new-data-localization-law

Regulations on the Administration of Internet Publishing Services and the *Promulgation of the Guidelines on Acceptance Inspection for Commencement of Business of Insurance Companies* mentioned above may also be interpreted to allow the overseas storage of the copies of data retained in China.

In the second layer, it is required that data can only be stored within the territory. Data processing can only be carried out in territory, but it can be accessed from abroad. For example, partial fields of data can be accessed from abroad instead of the whole: China's ***Administrative Regulations on Credit Investigation Industry*** requires that "the collation, preservation and processing of information collected in China shall be carried out in China", and there is no specific prohibition on the visit from abroad.

The third layer requires data storage, processing, and access to be carried out within the territory. This is the most stringent requirement. Article 77 of Australia's ***Personal Control Electronic Health Records Act*** mentioned above provides that: 1) records shall not be carried outside Australia, nor shall be held outside Australia; 2) all information relating to the records shall not be processed outside Australia.[59] Among them, "no holding records outside Australia" means that access from abroad is prohibited. Another example is the People's Bank of China for ***Banking Financial Institutions to Get the Personal Financial Information Protection Work Well Done***, which requires that "banking financial institutions shall not provide domestic personal financial information to overseas except as otherwise stipulated by laws and regulations and the people's bank of China". The "offer" includes requests for access from outside the country.[60]

4.3. Data Localization Coverage

As far as the author is aware of, no country requires all electronic data to be stored locally. Most countries choose to define the categories and types of data to be stored locally. The common types are as follows:

Personal data (or personal information). This is also the most common data type required for data localization.

Important data in the industry. For example, healthcare industry (such as Australia), banking industry (such as China), insurance industry (such as China), credit investigation industry (such as China), transportation industry (such as China), electronic payment industry (such as Turkey [61]), map data (such as South Korea [62]), network information service (such as Vietnam [63]), etc.

59 Full text of Australia's *Personal Control Electronic Health Records Act*, see https://www.legislation.gov.au/Details/C2012A00063

60 See evidence to support such understanding, the people's bank of China Shanghai branch on the banking financial institutions to do a good job of personal financial information protection issues related to notice (Shanghai silver hair [2011] no. 110) in the "four, about the banking financial institutions to provide personal financial information abroad" answer: "notice" stipulated in article 6: "except as otherwise provided in laws and regulations and the people's bank of China, the banking financial institutions shall not be provided to foreign domestic personal financial information." Where a domestic banking financial institution is required to provide domestic personal financial information to an overseas head office, parent bank, branch or sub-bank with the written authorization or consent of the customer, it shall not be deemed as violating the regulations. A banking financial institution shall guarantee the confidentiality of the personal financial information obtained by its head office, parent bank, branch or subsidiary abroad. For the full text of the document, please refer to the "Peking University Law" database, http://www.pkulaw.cn

61 Article 23 of "*Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions*" in Turkey. For the full text of the document, see: https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf

62 Chander, Anupam and Uyen P. Le, 2015, "Data Nationalism", Emory Law Journal, v. 64, pp.677-739. P.704.

63 Vietnam "Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and useof Internet services and online information Article 24. For the full text, see https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF

4.4. Exemption Conditions of Data Localization

While many countries require data to be stored locally, exemptions are explicitly listed. Therefore, the difficulty of meeting the exemption conditions is also an important indicator of the severity of localized data storage. Based on comprehensive analysis, exemption conditions mainly exist in the following situations: **The data subject shall give express consent:** South Korea, India and Brazil[64] are mentioned above.

Data recipients outside the territory shall be able to provide data protection at a level comparable to that of the territory. The most typical examples of this situation are the EU's common data protection regulations mentioned above and Canada's cross-border personal data processing guidance. This is currently the most common exemption for the cross-border transfer of personal data. According to the author's incomplete statistics, at least 28 member states of the European Union, as well as all states granted with "adequacy" status by the European Commission, including Australia[65], China's Hong Kon[66], Argentina[67], Israel[68], Japan[69], New Zealand[70] and Singapore[71] have adopted such exemption conditions.

Discretion of the public authority. In this case, the discretion of the public authority plays a decisive role in whether the data can flow across the border or even go beyond the provisions of established basic principles. For example, the Article 129 in Malaysia's Personal Data Protection Act, which came into effect in 2013, requires that the basic principle for the transmission of citizens' personal data abroad is that the country where the data is received should be able to provide a level of data protection comparable to that of the local country. However, article 46 of the act provides that the minister of the competent authority may exempt a single data subject or a type of data subject from the protection of the principles or provisions of the personal Data Protection Act and may attach any conditions to the exemption.[72] As a result, the minister of the competent authority has considerable discretion over the transmission of specific data abroad. Similarly, Singapore's Personal Data Protection Act, which came into force in 2014, requires overseas data recipients to provide data protection at the same level as local data protection in principle in article 26, but at the same time gives Singapore's "Personal Data Protection Commission" extensive discretion. The committee may, upon the agency's application, waive in writing the agency's obligation to comply with cross-border data compliance and may, in its judgment, attach any conditions.[73]

64 DLA Piper, 2016, Data Protection Laws of the World. P53. https://www.dlapiperdataprotection.com/#handbook/world-map-section

65 The Federal Privacy Act 1988 and its Australian Privacy Principles especially "Australian Privacy Principle 8 — cross-border disclosure of personal information" https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles#australian-privacy-principle-8-cross-border-disclosure-of-personal-information

66 The Office of the Privacy Commissioner for Personal Data of Hong Kong, 2014, "Guidance on Personal Data Protection in Cross-border Data Transfer", https://www.pcpd.org.hk/english/news_events/media_statements/press_20141229.html It is important to note that the current section of Hong Kong's personal data protection law regulating cross-border data transfers has not yet taken effect.

67 DLA Piper, 2016, Data Protection Laws of the World. P21

68 Same as above, P212.

69 Same as above, P229.

70 Same as above, P327.

71 Same as above, P404.

72 *The personal Data Protection Act,* full text in Malaysia, see www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf

73 *The personal Data Protection Act,* full text in Singapore, see https://www.pdpc.gov.sg/legislation-and-guidelines/legislation

There are similar cases in China where public authorities are given discretion. The provisions of the ***Notice of the People's Bank of China for Banking Financial Institutions to Get the Personal Financial Information Protection Work Well Done*** in 2011 mentioned above requires that: Unless otherwise prescribed by any law or regulation or the People's Bank of China, the banking financial institution shall not provide any domestic personal financial information to an overseas party". The Shanghai branch of the people's bank of China explained the above provisions in its " ***Notice of the People's Bank of China for Banking Financial Institutions to Get the Personal Financial Information Protection Work Well Done*** " (Shanghai Yinfa [2011] no. 110): "Where a domestic banking financial institution is required to provide domestic personal financial information to an overseas head office, parent bank, branch or sub-bank with the written authorization or consent of the customer, it shall not be deemed as violating the regulations".[74] It can be seen that the right to interpret the exemption is not only in the people's bank of China itself, but also in the Shanghai branch authorized by the people's bank of China.

5. The "reasonable limitation" principle for the local storage of data

The above difficulties of approaching and applying data localisation policies translate into significant application difficulties for data administrators, data controllers and processors. These are often left without guidance when deciding which provisions to apply on their databases and data processing practices. However, it is these actors that are the actual recipients of data localisation provisions. To this end, taking into account the above analysis, a principle of "reasonable limitation for the local storage of data" is suggested in this paper; whenever in doubt, administrators, controllers and other decision-making parties could revert to it when making decisions on their data.

5.1. A spin-off of the principle of proportionality in the data localization domain

Because of the intervention of national data sovereignty, arrangements for the cross-border data flow that should have been formed between private entities in specific scenarios will be required to be kept locally or only if the exemption conditions set by national data sovereignty are met can the data flow across borders. Undoubtedly, data localization is a manifestation of the public power of the state. The principle of proportionality is the "imperial clause" that must be observed when the public power is exercised,[75] its requirements on the necessity, appropriateness and balance of purpose and means are of great guiding significance for governing data localization according to law and setting reasonable limits for it.

The principle of proportionality can be divided into three sub-principles: the principle of appropriateness, the principle of necessity and the principle of balance: The principle of appropriateness means that the means of the act of public power should contribute to or be able to achieve the

74 Notice of the people's bank of China Shanghai branch on issues related to the protection of personal financial information by banking financial institutions, the full text of which can be found in the "Peking University Law" database, http://www.pkulaw.cn

75 Hu Jinguang, *China's social imperative - to put public power into institutional cage*, *The Zi guang ge*, 2014(7):pp79-80. http://cpc.people.com.cn/n/2014/0714/c68742-25279102.html Also see Wang yaqin: *the proportion principle of the German public law*, *Study Times*, 2014(11), A2 version. http://dzb.studytimes.cn/shtml/xxsb/20141103/7630.shtml .

goal pursued. The principle of necessity refers to the principle that among the numerous means to achieve the goal "equally effectively", the means adopted by the act of public power should cause the least damage. The principle of balance requires that the public interest enhanced by the means of public power act should be proportional to the damage caused.[76]

The following section examines the relationship between the value objectives and regulatory means of data localization using the principle of proportionality. According to the requirement of appropriateness and necessity in proportional principle, the "reasonable limit theory of data localization" is constructed. Due to the requirement of balance in the principle of proportionality, it is necessary to get rid of the relationship between the narrow sense of ends and means, list the ends as the objects of examination and measurement, and ask whether it is reasonable to ask someone or someone to bear a specific burden for a specific purpose.[77]

5.2. Assessing the appropriateness and necessity between the purpose and the means

5.2.1. Data Security and data localization

According to the principle of necessity under the principle of proportionality, it is necessary to improve the security level of data by limiting the storage place of data. But many studies have shown that data security does not actually depend on where the data is stored, but rather on how it is stored and transmitted. [78]

First of all, data security is nothing more than the result of the comparison of forces between attack and defense. At this stage the offensive is showing an overwhelming advantage.[79] For hackers and criminal organizations, they will use every possible means as long as the data are targeted no matter where they are stored, such as the use of phishing, trojans, viruses and other technical means, or directly bribe the internal staff. They do not abandon an attack because of geographical restrictions, and the nature of the Internet allows them to easily carry out cross-regional attacks. [80]

So, from a national security's point of view, might it make sense to force the data to be local? After all, the data remains in the country, and the network security authorities can force the owners or operators of information system to take adequate or additional security measures at their own discretion. But even in this sense, data localization could not be necessary. Because when the data needs to be transmitted abroad, the data exporter can "transmit" the additional security obligation imposed by the domestic competent authority to the overseas data receiver through

76 Representative works, see Yu lingyun: *The Principle of Proportionality in Administrative Law*, *Jurist*, 2002 (2). Jiang hongzhen: *Study on The Principle of Proportion -- Judicial Evaluation of The Choice of Government Regulation Tools*, *Law Press*, 2010. Yang dengfeng: "*From The Reasonable Principle to The Unified Proportion Principle*", *China Law*, 2016(3). Liu quan: *Reconstruction of The Principle of Legitimacy of Purpose And Proportion*, *China law*, 2014(4).

77 Yang dengjie, "*The Principle of Constitutional Proportion of Executive Power in China And Comparison with The Multiple Review Benchmark in The United States*", *Chinese And Foreign Jurisprudence*, 2015(2), page 372.

78 Mirko Hohmann, Tim Maurer, Robert Morgus and Isabel Skierka, 2014, "Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013", P4, http://www.gppi.net/publications/global-internet-politics/article/technological-sovereignty-missing-the-point/

79 See Hong yanqing: "*Regulation Based on Management" -- Reconstruction of Network Operators' Security Protection Obligation, global law review*, 2016(4), pp.28-33.

80 See Chander, Anupam and Uyen P. Le, 2015, "Data Nationalism", Emory Law Journal, v. 64, pp.718-721.

contract and other forms as the precondition for the cross-border transmission of data. In this way, security measures follow the data all the way from the border to the border.

Some people may think that, from the perspective of criminal investigations, data localization can enable law enforcement agencies to obtain the jurisdiction of the cases, which is a deterrent to hackers and criminals, and thus the risk of attack can be reduced. The difficulty of detection often rises sharply when it comes to overseas investigation and evidence collection, time-consuming and laborious bilateral judicial cooperation procedures. This, however, is not necessarily the case. First of all, the jurisdiction acquired by investigation organ is no need to rely solely on data obtained in the territory.[81] Secondly, even if domestic authorities gain jurisdiction through data localization, their deterrent power against hackers and criminals is limited in many cases. Domestic hackers and criminals especially who are experienced basically use foreign servers as a springboard to create the illusion of overseas attacks.

Of course, the above analysis is only from theoretical level. In practice, the cross-border transmission of data often means the increase of links in the data chain. From a common sense, it means that the risk of errors is increasing, and the possibility of confidentiality, integrity and usability being damaged is increasing. Perhaps data localisation can reduce the risk to some extent. However, it should also be borne in mind that even if data storage and transmission are confined to a single country, these risks are not necessarily lower than those associated with cross-border data transmission, as the awareness of the high risks associated with cross-border data transmission may prompt data exporters to take additional security measures.

5.2.2 Protection of personal data and data localisation

The scope and degree of the right to self-determination of personal information, as well as the obligations undertaken by data controllers and other relevant parties to meet the right to self-determination of personal information are often the choices made by a country when balancing the interests of the following three aspects:
Interests in self-determination of personal information: including control over the collection, use, sharing and disclosure of personal information to a certain extent, as well as controlling the impact on individuals brought by;
Development interests: reasonable demands of enterprises and industries to make full use of personal information to provide, improve and innovate products and services;
Public interest: government departments use personal information to complete public management, as well as the free flow of information and the public's right to know necessary for social development.

Obviously, each country makes different choices when balancing competing interests. Therefore, from the perspective of personal data protection, data localization can ensure the rights of individuals, the obligations of data controllers and other relevant parties, etc., and can follow the specific balance of interests made by this country. [82]

81 See article 8 in China's "criminal law": "This law may be applied to any foreigner who commits a crime against the state or a citizen of the People's Republic of China outside the territory of China and whose minimum punishment prescribed by this law is fixed-term imprisonment of not less than three years, except where no punishment is imposed in accordance with the law of the place where the crime was committed".
82 As mentioned earlier, the EU gives individuals the right to be forgotten, while the right to be forgotten is less recognized in the United States.

However, it should be noted that data transmission to foreign countries can still enjoy the same level of security, the right to self-determination of personal information configuration and so on with local level by the contract, the company's internal guidelines and other forms. Therefore, as a result, virtually every country also allows this exemption from the requirement for data localization.

In general, at the level of data protection, the main significance of data localization is to ensure that the configuration arrangements made by the country in respect of the right to self-determination of personal information, the obligation of data controllers and other relevant parties to meet the right to self-determination of personal information can be applied to specific data, rather than to protect data security.

Nevertheless, in the cyber world, it is mainly hostile countries or hostile forces with national backgrounds that can threaten national security. At present, various hacker organizations with national backgrounds have launched many advanced persistent threats (APT) against organizations and institutions in China.[83] These examples show that even mandatory data localization in a country cannot avoid the hands of hostile countries or hostile forces with national background. Therefore, as far as data security is concerned, mandatory localization cannot actually guarantee data security.

However, mandatorily data localized can indeed eliminate a certain kind of risk -- overseas countries can legally and secretly obtain data transmitted to their territory, especially sensitive data, by legal and administrative means. In the "prism" program exposed by Snowden, the United States made use of the advantage that most of the data transmitted through the Internet would pass through the territory, so that the United States security agency could directly intercept a large amount of data. At the same time, the security agency legally and secretly required the American Internet companies to cooperate with it, and obtained a large amount of user data both at home and abroad. In this case, the U.S. government successfully monitored the world by exercising sovereignty over its own data cables and data centers.[84] As a result, after the "prism" exposure, Germany and other European countries immediately put forward a plan to establish their own email system and cloud data center, not through the United States optical cable and other technical means.[85]

Coupled with the description model of data localization severity model in Part IV, it also can be concluded that in order to meet the requirements of data security and personal data protection by data localization, it is not necessary for national sovereignties to actually participate in each

83 Tianyan laboratory, Ocean Lotus (sea lotus) APT report summary. In the report, the 360 company's security team revealed a hacker groups outside of the Chinese government, research institutes, maritime agency, marine construction, shipping companies and related important areas for organized, planned, targeted long uninterrupted attack on http://blogs.360.cn/blog/oceanlotus-apt/ since April 2012. See also the APT report of the 360 day team: mahagrass organization (apt-c-09), an offshore APT organization from South Asia that has been active for seven years. The mahagrass group conducts cyber espionage against China, Pakistan and other Asian countries, mainly to steal sensitive information. The attacks, which date back to November 2009, are still active. In the attacks against China, the group mainly targets government institutions and the field of scientific research and education. http://bobao.360.cn/learning/detail/2935.html .

84 Lorenzo Franceschi-Bicchierai, "The 10 Biggest Revelations From Edward Snowden's Leaks", Jun 05, 2014, http://mashable.com/2014/06/05/edward-snowden-revelations/#NSc.Xn8fSiq2

85 Various Technological measures proposed by the European side, see Mirko Hohmann, Tim Maurer, Robert Morgus and Isabel Skierka, 2014, "Technological double: Missing the Point? An Analysis of European Proposals after June 5, 2013 ",

scene. All they need to do is setting the principle or basic conditions of cross-border transmission of data, rights and obligations by rules for each private subject involved in advance. In specific scenarios, private subjects know their respective rights, obligations and the conditions for cross-border transmission in advance. As long as the agreed data transmission arrangement "passes the threshold", the transmission can be carried out.

6. A policy-making tool and an implementation mechanism for data localisation requirements

In view of the above analysis, applying the reasonable limitation principle for the local storage of data and the data localisation severity model analysis, at a policy-making level the following criteria should be taken into consideration when deciding whether to apply data localisation:

- Taking into consideration the degree of necessity of localized data storage;
- The goal to be achieved by the "reasonable limitation" principle for the local storage of data" is to minimize, whenever possible, the data localisation severity model;

DATA LOCALISATION LEVELS

- National level data security + data control right + prevent the sensitive data from malicious use and threat to national security High Direct involvement of sovereignty + assessment case by case + wide coverage + Absolute localized storage High
- Personal data protection data security + personal information self-determination right + the obligation of data controller and relevant partiess to satisfy the self-determination right Medium Sovereignty integrated into private right + prior design + personal data + medium localized storage Medium
- Data security Confidentiality + Integrity + Availability Low Sovereignty integrated into private right + prior design + wide coverage + low localized storage Low

Similarly, once data localisation policy options are in place the following steps could be applied by data administrators, controllers and processors:

- Entities and organizations evaluate the businesses and data to be transmitted cross-border;
- Governmental agencies in charge assess the evaluation reported prepared by the entities and organizations;
- The degree of necessity of localized data storage is assessed

The first is the assessment process. At the very beginning, organizations with cross-border data transmission needs shall conduct self-evaluation and propose supporting safeguard measures (" step 1 ") according to the "reasonable limit theory of localized data storage", and submit the evaluation results and supporting safeguard measures to the competent authorities (" step 2 "). Secondly, the competent authorities should review the evaluation report and supporting safe-

guard measures in accordance with the "reasonable limit theory of localized data storage" and make their own judgment (" step 3 "). Finally, they should ask the organization to form specific arrangements for cross-border data transmission according to the requirements of the competent authorities (" step 4 ").

The second is the substance of the evaluation. If the assessment shows that the data only involves data security, the public authority shall adopt the mode of "light supervision", set the rights and obligations of each private subject, and list the cross-border principles and "threshold" in advance. After meeting the above conditions, the public authority may release the data. If the assessment shows that the data involves the protection of personal data, the public power also achieves the regulatory purpose by means of the rights and obligations of each private subject in advance and the cross-border principle. However, in order to protect the right of self-determination of personal information, the threshold is higher than the data security. If the assessment shows that the data is related to national security, the public authority has the right to carry out "strong supervision", discuss one case at a time, directly involve in specific scenarios, participate in the design of specific cross-border data safeguard measures, or require the data to be stored locally if the risk cannot be controlled.

To sum up, the biggest advantage of establishing a security assessment method for cross-border data transmission based on the "reasonable limit theory of data localization" proposed in this paper is that it can run through the spirit of the principle of proportionality in the process of supervising cross-border data and strike a balance between security and development.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri & Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommuni-cations operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou & Paul de Hert (14 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou & Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

BRUSSELS PRIVACY HUB