Data Transferability in Mainland China

Dr. Tianxiang HE
School of Law, City University of Hong Kong

at

The 11th IP Conference, CUHK, 2 August, 2019

RCCL'S CONTRACT RESEARCH FOR MICROSOFT HONG KONG LIMITED —

"LEGAL RESEARCH PROJECT: PROPOSAL FOR HONG KONG TO BE A DATA CENTRE HUB FOR THE GREATER BAY AREA & CHINA"

Team Members:

Dr. Lei CHEN	*Associate Dean & Associate Professor; Director, Centre for Chinese and Comparative Law (RCCL), School of Law, City University of Hong Kong*
Dr. Chunyan DING	*Assistant Dean & Associate Professor; Core Member, Centre for Chinese and Comparative Law (RCCL), School of Law, City University of Hong Kong*
Dr. Tianxiang HE	*Assistant Professor; Affiliated Member, Centre for Chinese and Comparative Law (RCCL), School of Law, City University of Hong Kong*
Prof. Pinxin LIU	*Professor, Renmin University of China School of Law*
Prof. Rostam J. NEUWIRTH	*Professor, Faculty of Law, University of Macao*

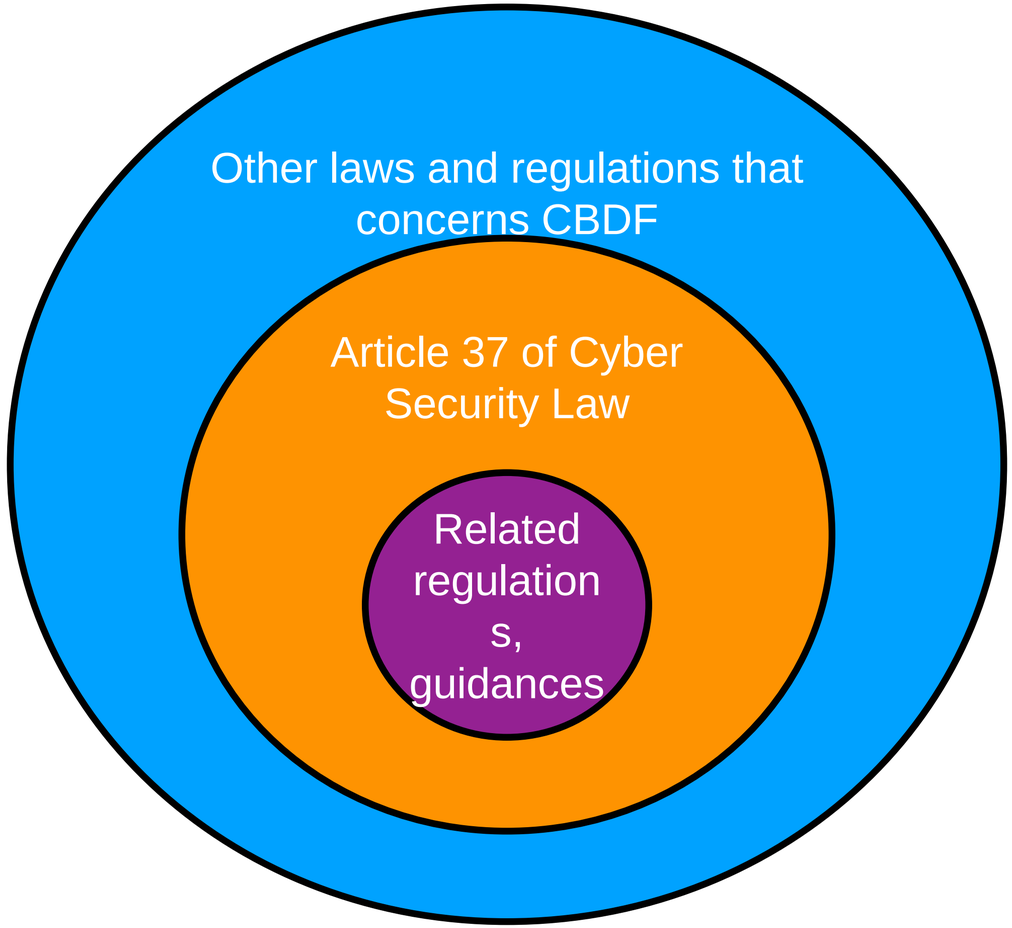
Background of CBDF

- ‘data is the new oil’

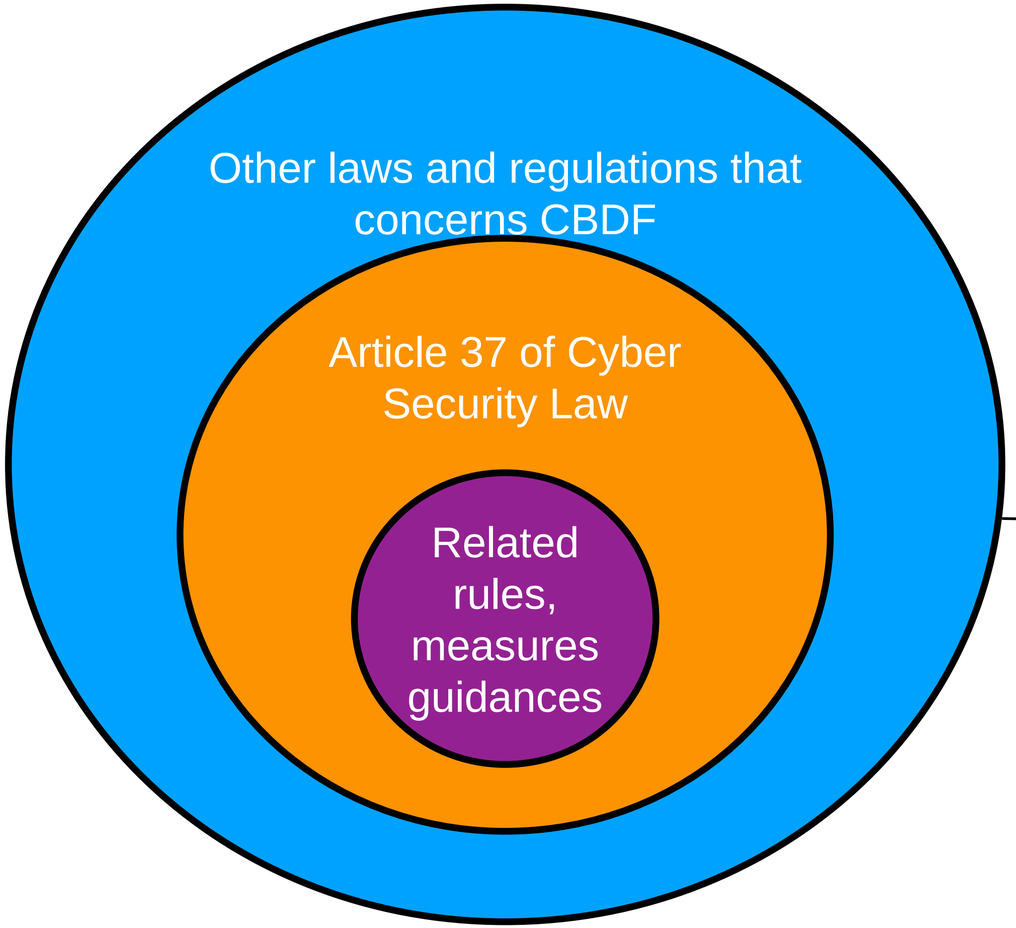
- cross-border data flow (跨境數據流動, CBDF) not only forms a significant part of cyberspace regulation in every country; it is also the crucial content in every country’s assertion of its cyber sovereignty.

- China was a latecomer on cross-border data flow regulation. But China possesses advantageous conditions for enacting such kind of legislation: The large-scale digital economy market, the open and vibrant policy environment, and the unique “one country, two systems” setting, all these factors are advantageous to China’s exploration of the establishment of its cross-border data flow system.

Legislative overview



Legislative overview



- Article 37 of the Cyber Security Law (《網絡安全法》)
- the Archives Law (《檔案法》), the Law on Guarding State Secrets (《保守國家秘密法》), the Measures for the Administration of Population Health Information (《人口健康信息管理辦法》and the Regulation on Map Management (《地圖管理條例》) .
- Guide to the Personal Information Security Impact Assessment (Draft for Comments) (《信息安全技術 – 個人信息安全影響評估指南（徵求意見稿）》) , the Critical Information Infrastructure Security Protection Regulations (Draft for Comments) (《關鍵信息基礎設施安全保護條例（徵求意見稿）》) and the Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (《信息安全技術 – 數據出境安全評估指南》

Laws

Name of Statutory Document	Effective Date	Provisions
Cyber Security Law	1 June 2017	Article 37, Article 31, Article 66
General Provisions of the Civil Law	1 October 2017	Article 127
Criminal Law (2017 Amendment)	4 November 2017	Article 253(1)
National Security Law	1 July 2015	Article 25
Law on Guarding State Secrets	29 April 2010	Article 25, Article 48
Archives Law	7 November 2016	Article 16, Article 18, Article 24, Article 25
Counterterrorism Law	27 April 2018	Article 19
International Criminal Justice Assistance Law	26 October 2018	Article 4
Decision on Strengthening Information Protection on Networks	28 December 2012	

Judicial Interpretation

- The Supreme People's Court and the Supreme People's Procuratorate jointly issued the Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information (《關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》). Article 1 of the Interpretation provides that:

  - **"Citizens' personal information"** as prescribed in Article 253A of the Criminal Law means all kinds of information recorded in electronic form or any other form, which can be used, independently or in combination with other information, to identify a specific natural person's personal identity or reflect a specific natural person's activities, including the natural person's name, identity certificate number, communication and contact information, address, account password, property status, and whereabouts, among others.

Administrative Rules

- Article 24 of the Regulation on Map Management (《地圖管理條例》): no entity or individual may carry or mail any map in non-compliance with relevant standards and provisions of the state in or out of China.

- Article 24 of the Regulation on the Administration of Credit Investigation Industry (《徵信業管理條例》): for information collected inside China, credit investigation institutions shall arrange, save and process it inside China.

- Article 21 of the Regulation on the Implementation of the Law on Guarding State Secrets (《保守國家秘密法實施條例》): where state secret carriers are to be carried out of China, approval and carrying formalities shall be undergone according to the secrecy provisions of the state.

Departmental Rules Level

Issuing Body	Name of Statutory Document	Effective Date	Major Contents and Provisions
State Administration of Press, Publication, Radio, Film and Television & Ministry of Industry and Information Technology	**Provisions on the Administration of Online Publishing Services (《網絡出版服務管理規定》)**	10 March 2016	Article 8
People's Bank of China (中國人民銀行)	**Notice on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information**	1 May 2011	Personal financial information acquired inside China shall be stored, processed and analyzed inside China. (Article 6)
Ministry of Transport, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Commerce, State Administration for Industry and Commerce (Abolished), General Administration of Quality Supervision, Inspection and Quarantine (Abolished) & Cyberspace Administration of China	**Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (《網絡預約出租汽車經營服務管理暫行辦法》)**	1 November 2016	An online taxi booking platform company shall observe the relevant state provisions on network and information security and the personal information collected and business data formed shall be stored and used in the Chinese mainland. (Article 27)
Ministry of Industry and Information Technology (工業和信息化部)	**Provisions on Protecting the Personal Information of Telecommunications and Internet Users**	1 September 2013	Article 4, Articles 8, 9, 10
National Archives Administration (國家檔案局)	Measures for the Implementation of the Archives Law of the People's Republic of China	1 March 2017	Article 18
Ministry of Finance (財政部), National Archives Administration	**Measures for the Administration of Accounting Archives (2015 Amendment)**	1 January 2016	Article 25
Ministry of Finance	**Interim Provisions on Accounting Firms' Provision of Auditing Services for the Overseas Listing of Enterprises in Chinese Mainland**	1 July 2015	Article 5, Article 12
National Health and Family Planning Commission (國家衛生和計劃生育委員會) (Abolished)	**Measures for the Administration of Population Health Information (For Trial Implementation)**	5 May 2014	Article 9, Article 10
National Health Commission (國家衛生健康委員會)	Measures for the Administration of the Standard, Security and Service of National Health and Medical Big Data (For Trial Implementation)	12 July 2018	Article 30
Ministry of Science and Technology (科學技術部) and Ministry of Health	Interim Measures for the Administration of Human Genetic Resources	10 June 1998	Article 4, Article 6, Articles 11, 12, 13, 14, 15 and 16, Articles 21 and 22
Cyberspace Administration of China	Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data (Draft for Comments)	Not yet come to effect	
	Critical Information Infrastructure Security Protection Regulations	Not yet come to effect	Chapter 3, Article 29, Article 34, Article 46

National Standard Level

Document Name	Effective Date	Major Contents and Provisions
Information Security Technology – Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems	1 February 2013	Section 5.4.5
Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)	Not yet come to effect	This standard provides for the process, major points and method of security assessment of cross-border transfer of personal information and important data.
Information Security Technology – Guide to the Personal Information Security Impact Assessment (Draft for Comments)	Not yet come to effect	This standard sets out the basic concepts of personal information security impact assessment, its structure, method and process.
Information Security Technology – Guide for De-Identifying Personal Information (Draft for Comments)	Not yet comet to effect	This standard describes the goal and principle of de-identification of personal information, and the process of de-identification and the relevant administrative measures. This standard provides specific guidelines regarding de-identification of personal information for micro data, which applies to (persons/organizations) who handles personal information; it also applies to the work of personal information security supervision and management and assessment by departments related to network security and third-party assessment institutions.
Information Security Technology – Guidelines for Security Inspection and Evaluation of Critical Information Infrastructure (Draft for Comments)	Not yet come to effect	Critical information infrastructure (Section 3.1); Situation of protecting personal information and important data in compliance examination (Section 7.2.5)
Information Security Technology – Security Controls of Critical Information Infrastructure (Draft for Comments)	Not yet come to effect	Critical information infrastructure (Section 3.1) Classification of data (Section 5.1.2); Compliance requirements of classified protection (Section 6.1); Data protection (Section 6.4)
Information Security Technology – Basic Requirements for the Protection of Network Security of Critical Information Infrastructure (Draft for Comments)	Not yet comet to effect	Section 3.1; Section 4.2.8
Information Security Technology — Indicator System of Critical Information Infrastructure Security Assurance	Not yet come to effect	Critical information infrastructure (Section 3.1)

Analysis of the Significant Normative Documents: The Cyber Security Law

The Cyber Security Law is the first piece of basic legislation on cyber security in mainland China, and it sets out the basic framework of cyber security legislation for the country. The Cyber Security Law was passed on 7 November 2016 and came into force on 1 June 2017.

HACKING INTO CHINA'S CYBERSECURITY LAW

*Jyh-An Lee**

China's Cybersecurity Law, which is thus far the most important internet legislation to be passed in the country, came into effect on June 1, 2017. The law has attracted significant attention and criticism from foreign companies. Although the Chinese government claims that the Cybersecurity Law will help reduce the risk of cyberattacks and safeguard national security, some critics believe that the law will further erode internet freedom in China. In particular, concerns have been raised that the law may not effectively enhance China's current level of cybersecurity but instead may be used to facilitate government censorship and surveillance, to increase unnecessary business operating costs, to steal intellectual property from foreign companies, and to protect domestic industries from global competition.

This Article provides a thorough analysis of important provisions of the Cybersecurity Law as well as their policy implications. It views the Cybersecurity Law as part of a broader set of policy steps that have been taken to streamline laws concerning the internet and national security. The law

* Associate Professor, Faculty of Law, The Chinese University of Hong Kong. I would like to thank Rehan Abeyratne, Gillian Bolsover, Anatole Boute, Bernard Chao, Shun-Ling Chen, Yu-Jie Chen, Wen-Tsong Chiou, David Donald, Yu Hong, Stuart Hargreaves, Gus Hurwitz, Lianrui Jia, Min Jiang, Jae Woon Lee, Wanbil Lee, Yu-Hsin Lin, Tzu-Yi Lin, Noam Noked, Tokunbo Ojo, Jeffrey Ritter, Lotus Ruan, Dini Sejko, Hsi-Ping Schive, Yen-Tu Su, Dicky Tsang, Felix Wu, Dwayne Winseck, Peter Yu, and Wolfgang Zankl for their helpful comments. This Article has also benefited from feedback provided in the 2017 Internet Law Works-in-Progress Conference at Santa Clara Law School, the 15th Chinese Internet Research Conference: "Divergence and Convergence in China's Internets" at Texas A&M University School of Law, Faculty Seminar at the Institutum Iurisprudentiae, Academia Sinica (IIAS) in Taipei, Faculty Research Seminar at The Chinese University of Hong Kong Faculty of Law, "iEthics-Cyberport Symposium on Data Privacy Protection and Cybersecurity" in Hong Kong, and the "Global Media Forum: Changes and Adaptations: Chinese Media and its Global Development" workshop at York University in Toronto. I also thank Agnes Cheung, the Legal Resources Librarian for her invaluable assistance. I am grateful to the editors of the *Wake Forest Law Review* for their extraordinary editorial support. The study underlying this Article was supported by a grant from the Research Grants Council in Hong Kong (Project No.: CUHK 14612417)

Article 37 of the Cyber Security Law

- Personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of the People's Republic of China shall be stored within China. If it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.

- "关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。"

purpose

- to protect the security of the network; to maintain the sovereignty of the cyberspace, national security and public interest; to protect the legal rights of citizens, legal persons and other organizations, hence enhancing the healthy development of informatization of the economic society.

- the second level of the purpose of its enactment is to maintain the security of the operation of the critical information infrastructure.

- to protect personal information and important data

Content

- (1) The subjects of liability are the operators of the critical information infrastructure but not all network operators;

- (2) The targets of protection are the personal information and important data collected and produced by the subjects of liability during their operations within the territory of the People’s Republic of China;

- (3) The content of liability is storing the information/data within China;

- (4) Cross-border transfer of relevant personal information and important data out of China must comply with two conditions, namely the relevant business requirements and passing the security assessment.

Article 31 of the Cyber Security Law

- The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the **critical information infrastructure** in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the **critical information infrastructure** that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council.

- "国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。"

- The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

- "国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。"

Article 31 of the Cyber Security Law

- The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the **critical information infrastructure** in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the **critical information infrastructure** that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council.

- "国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。"

- The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

- "国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。"

Article 31 of the Cyber Security Law

- The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the **critical information infrastructure** in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the **critical information infrastructure** that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council.

- "国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。"

- The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

- "国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。"

Article 66 of the Cyber Security Law

- Where a critical information infrastructure operator stores network data overseas, or provides network data to the overseas in violation of Article 37 of this Law, the competent department shall order it to take corrective action, give it a warning, confiscate its illegal income, and impose a fine of not less than 50,000 yuan but not more than 500,000 yuan on it, and may order it to suspend relevant business operation, cease business operation for rectification, or close down the website, or may revoke the relevant business permit or business license, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons.

- “关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

Critical Information Infrastructure Security Protection Regulations (Draft for Comments) 关键信息基础设施安全保护条例（征求意见稿）

- Article 18 of the Regulations provides that:

- Network facilities and information systems operated and managed by the Entities (danwei) listed below, if being destroyed, loses functions or encounters data leakage will result in serious damage to state security, the national economy and the people's livelihood and public interest, should be brought into the scope of the protection of critical information infrastructure:

  1. Governmental agencies and Entities (danwei) which are in industry sectors and fields such as energy, finance, transportation, water conservancy, hygiene and medical care, education, social insurance, environmental protection, and public utilities;

  2. Information networks such as telecommunications networks, television broadcast networks and the Internet, and Entities (danwei) which provide cloud computing, big data and other large-scale public information network services;

  3. R&D and manufacturing Entities (danwei) which are in industry sectors and fields such as science and technology for national defense, large equipment manufacturing, chemicals, and food and drug;

  4. News organizations (danwei), such as broadcasting stations, television stations and news agencies; and

  5. Other critical organizations (danwei).

- “下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；（四）广播电台、电视台、通讯社等新闻单位；（五）其他重点单位。”

Critical Information Infrastructure Security Protection Regulations (Draft for Comments)

- **Article 19** of the Regulations provides that:
- The national cyberspace administration departments will, acting jointly with departments such as the telecommunications authority and the public security department of the State Council, formulate guidelines for identifying critical information infrastructure.
- The national industry regulatory or supervisory departments will, in accordance with the guidelines for identifying critical information infrastructure, identify critical information infrastructure within their own industry sectors and their own fields, and report the results of their identification in accordance with procedures.
- In the course of identifying and recognizing critical information infrastructure, the role of relevant experts should be fully taken into account, to make the identification and recognition of critical information infrastructure more accurate, reasonable and scientific.
- “国家网信部门会同国务院电信主管部门、公安部门等部门制定**关键信息基础设施识别指南**。”
- “国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。”
- “关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。”
- **Article 20** of the Regulations provides that:
- Operators of critical information infrastructure which has been newly constructed or the operation of which has been suspended, or where a major change to the critical information infrastructure has occurred, should promptly report the relevant circumstances to the national industry regulatory or supervisory departments.
- The national industry regulatory or supervisory departments should promptly carry out an adjustment of their identification on the basis of the circumstances reported by the operator, and report the results of their adjustment in accordance with procedures.
- “新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。”
- “国家行业主管或监管部门应当根据运营者报告的情况及时进行识别调整，并按程序报送调整情况。”

Critical Information Infrastructure Security Protection Regulations (Draft for Comments)

- **Article 34** provides that:

- The operation and maintenance of critical information infrastructure should be carried out within the territory of China. When there is a veritable need to carry out remote overseas maintenance for reasons of business necessity, they should report it in advance to the national industry regulatory or supervisory departments and to the public security department of the State Council.

- “关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。”

Measures on Security Assessment of Cross-border Data Transfer of Personal Information (Draft for Comments) (个人信息出境安全评估办法（征求意见稿）)

- Issued by the Cyberspace Administration of China on June 2019.
- The major contents of the Assessment Measures include: rules for local storage and security assessment of personal information and important data; principles of data cross-border transfer security assessment; specific missions of various subjects in security assessment; contents of focused assessment of the security of data cross-border transfer; and situations where data cross-border transfer are prohibited.
- This provision extends the subject of liability from critical information infrastructure operators to cover also the ordinary network operators.

Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments) (信息安全技术　数据出境安全评估指南（征求意见稿）)

- It is a set of guidelines formulated by the National Information Security Standardization Technical Committee after the promulgation of the Cyber Security Law, focusing on dealing with data cross-border transfer security assessment.

- The Guidelines sets out the procedure of the data cross-border transfer security assessment, the major aspects of assessment, and the assessment methods, etc. Besides, it also gives explanations to some core technical terms relating to data cross-border transfer.

- There are two annexes to the Guidelines, namely **“The Guidelines for Identifying Important Data”** (《重要数据识别指南》) and **“The Measures for the Assessment of Security Risk of Cross-border Data Transfer of Personal Information and Important Data”** (《个人信息和重要数据出境安全风险评估办法》). These two documents are crucial to the actual implementation of the cross-border data flow system.

The Practical Need for Cross-border Data Flow

- Personal Communication
- Business Needs
  - Execution of Public Duties by the Public Institutions
  - Operation of the Private Business
- Scientific Research Activities
- Administrative Supervision Activities
- Litigation

China’s Regulative model of Cross-border Data Flow

- **Ground rule: Localization of Data Storage (**also have to ensure the controllable security at the stages of data analysis, process and disposal, etc.**)**
- **Data Restricted of Export**
  - approval of competent authorities (《保守国家秘密条例》《会计师事务所从事中国内地企业境外上市审计业务暂行规定》)
  - users’ consent (《关于加强网络信息保护的决定》)
  - security assessment (《网络安全法》第37条, 《国家健康医疗大数据标准、安全和服务管理办法（试行）》)
- **Data Prohibited of Export** (《地图管理条例》规定“不得携带、寄递不符合国家有关标准和规定的地图进出境”，《网络预约出租汽车经营服务管理暂行办法》规定“网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用”；《人口健康信息管理办法（试行）》规定了“不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器”。)
- **Free to Export**
  - Open data
  - Harmless data

China’s Regulative model of Cross-border Data Flow (cont.)

- **Prohibition of Inflow (Article 19 of Counterterrorism Law)**
- **Free to Inflow (mainly include data which allow public access within mainland China and data whose inflow will not threaten national security)**

效力	名称	生效时间	条款	规制对象	规制模式
法律	《网络安全法》	2017.6.1	第37条	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据	境内存储+限制出境（安全评估）
部门规章	《国家健康医疗大数据标准、安全和服务管理办法（试行）》	2018.7.12	第30条	健康医疗大数据	境内存储+限制出境（安全评估）
法律	《保守国家秘密法》	2010.4.29	第25条	国家秘密载体	禁止邮寄、托运； 携带传递需获批
行政法规	《中华人民共和国保守国家秘密法实施条例》	2014.3.1	第21条	国家秘密载体	限制出境（按照国家保密规定办理批准和携带手续）
法律	《反恐怖主义法》	2018.4.27	第19条	互联网上跨境传输的含有恐怖主义、极端主义内容的信息	禁止传播
法律	《档案法》	2016.11.7	第16条、第18条	集体所有的和个人所有的对国家和社会具有保存价值的或者应当保密的档案	禁止私自携运出境
行政法规	《地图管理条例》	2016.1.1	第24条	不符合国家有关标准和规定的地图	不得携带、寄递出境
部门规章	《会计档案管理办法(2015修订)》	2016.1.1	第25条	单位的会计档案及其复制件	限制出境
部门规章	《会计师事务所从事中国内地企业境外上市审计业务暂行规定》	2015.7.1	第5条、 第12条	境内形成的审计工作底稿	境内存放+限制出境（按照境内外监管机构达成的监管协议执行）
法律	《关于加强网络信息保护的决定》	2012.12.28	全文	公民个人电子信息	不得非法获取或非法提供给他人
部门规章	《网络出版服务管理规定》	2016.3.10	第8条	从事网络出版服务所需的必要的技术设备，相关服务器和存储设备	必须存放在境内
部门规章	《关于银行业金融机构做好个人金融信息保护工作的通知》	2011.5.1	第6条	在中国境内收集的个人金融信息	储存、处理和分析应当在中国境内进行
行政法规	《征信业管理条例》	2013.3.15	第24条	征信机构在中国境内采集的信息	整理、保存和加工，应当在中国境内进行，限制出境
部门规章	《网络预约出租汽车经营服务管理暂行办法》	2016.11.1	第27条	采集的个人信息和生成的业务数据	境内存储和使用，不得外流
部门规章	《人口健康信息管理办法（试行）》	2014.5.5	第10条	人口健康信息	不得在境外服务器存储，不得托管、租赁在境外的服务器
部门规章	《人类遗传资源管理暂行办法》	1998.6.10	第4条、第6条、第11-16条、第21-22条	人类遗传资源	未经许可不得擅自出口、出境； 国际合作项目须办理报批手续
法律	《国际刑事司法协助法》	2018.10.26	第4条	证据材料	非经主管机关同意，不得向外国提供

Thank you!

tianxhe2@cityu.edu.hk