Navigating China's Evolving Cybersecurity and Data Protection Rules

Yan Luo, Partner, Covington & Burling LLP
Stacey Steele, Interim Chief Privacy Officer, S&P Global

Cybersecurity and Data Privacy Regulatory Framework

Cybersecurity Law

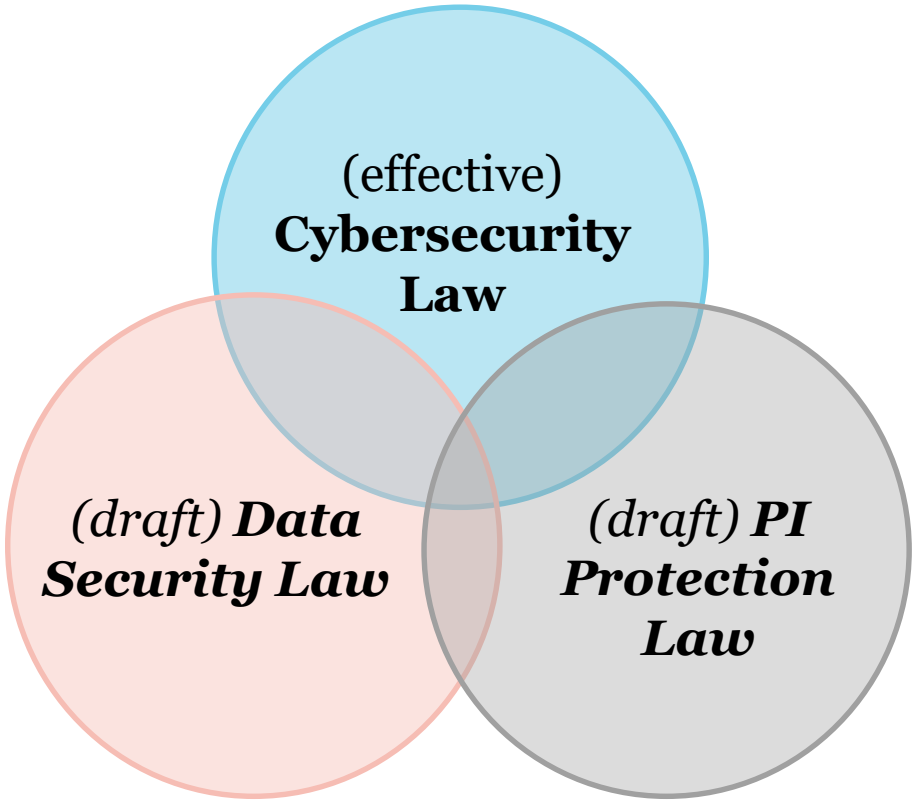
- Effective on June 1, 2017
- Fundamental law in cybersecurity and data privacy area.

Data Security Law

- Second draft issued for public comments on April 29, 2021
- Regulate data from a national security perspective, with a special focus on "important data".
- Expected to be finalized by the end of 2021.

Personal Information Protection Law

- Second draft issued for public comments on April 29, 2021.
- To be served as China's overarching privacy law moving forward.
- Expected to be finalized by the end of 2021.

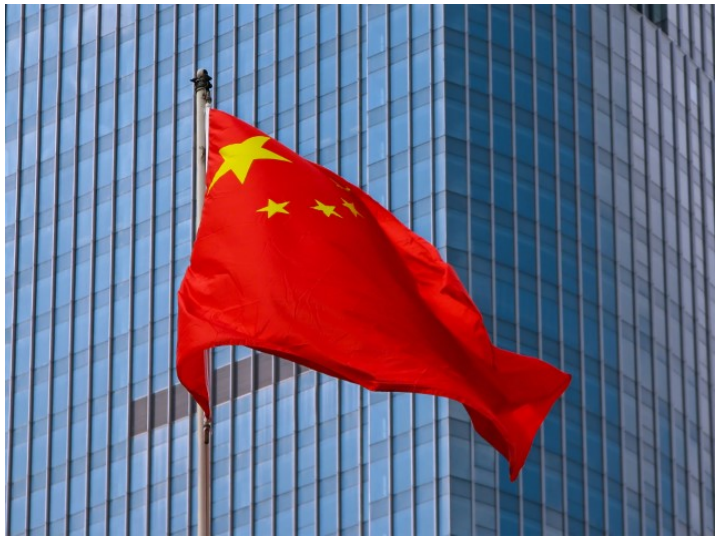


➢ **<u>Other laws and sectoral rules (e.g. Encryption Law, sectoral requirements in the financial and healthcare sectors)</u>**

Overview of Cybersecurity Law

China's Cybersecurity Law ("CSL")

- Imposes baseline data protection and cybersecurity obligations for "network operators," including complying with Multi-Level Protection Scheme ("MLPS") rules
- Provides a regulatory framework for operators of Critical Information Infrastructure ("CII")
- Stipulates a wide array of sanctions for non-compliant companies



Draft Data Security Law

Scope

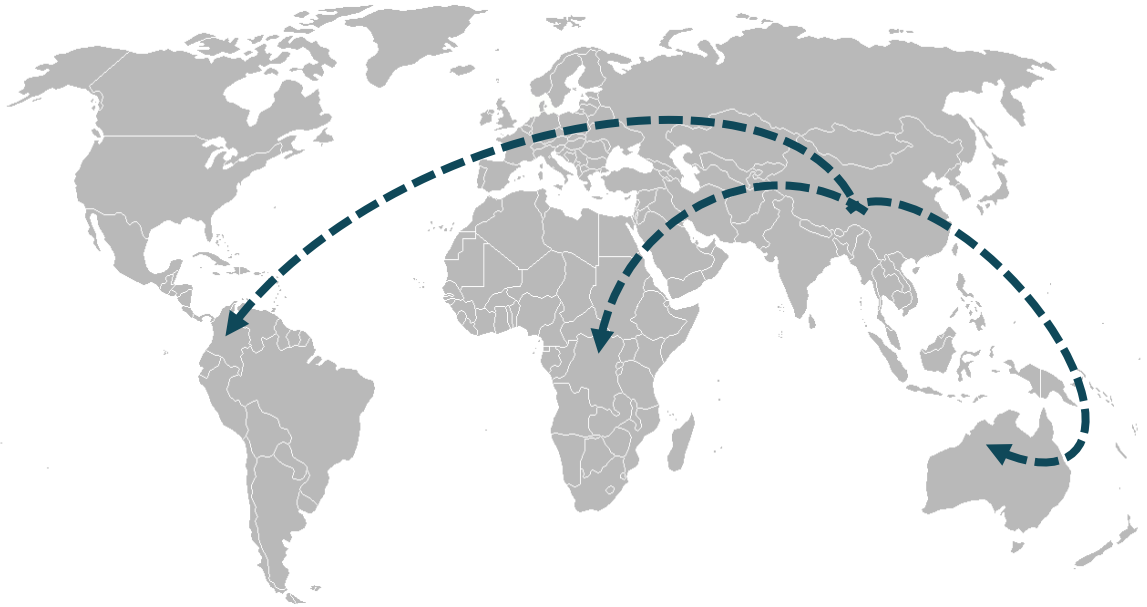
- Regulating "data processing activities" (i) within China and (ii) outside of China which may harm China's national security, public interests, or the rights of Chinese citizens or organizations.
- Introducing the concept of "important data"
  - Term itself not defined in the law
  - Central government has the mandate to issue the catalogue of "important data," while regional and sectoral agencies to release more detailed catalogues for their sectors/regions
  - Enhanced security protection for entities processing "important data"

Draft Data Security Law (Cont.)

- **Cross-border Transfer of Important Data**
  - Transfer by CII operators. CII operators must follow the rules established under the CSL.
  - Transfer by other data processing entities. Data processing entities that are non-CII operators are required to follow separate cross-border data transfer rules to be published by the Cyberspace Administration of China ("CAC") and other government agencies.

Draft Personal Information Protection Law

- **Extra-Territorial Effect**
  - Applies to the processing of personal information conducted outside of China, if the purpose of the processing is
    - to provide products or services to individuals in China;
    - to analyze or assess the behavior of individuals in China; or
    - for other purposes required by laws and regulations.
  - Offshore entities that process personal information of Chinese individuals shall establish a “dedicated office” or appoint a “representative” in China to be responsible for personal information protection in China.



Draft Personal Information Protection Law (Cont'd)

Legal Basis

Only process personal information with an appropriate legal basis.

The individual has given his or her **consent** to the processing

Necessary to enter into or perform a contract

Necessary to comply with a legal Responsibility or obligation

Necessary to respond to a public health emergency, or in an emergency to protect the safety of natural persons' health and property

To a reasonable extent, for purposes of carrying out news reporting and public opinion monitoring for public interests

Processing of personal information that is already made public and such a processing must be carried out for reasonable purposes in compliance with the law

Draft Personal Information Protection Law (Cont'd)

General Requirements for Cross-Border Transfer

- **Separate consent (if consent is the legal basis for processing)**
- **Prior risk assessment and record keeping**
- **Available transfer mechanisms:**
  - For CII operator and non-CII processing entities that process "large" volume of personal information (to be specified by CAC)
    - undergo a security assessment administered by CAC
  - If a security assessment is not mandatory
    - obtain certification from "professional institutions" in accordance with the rules of CAC
    - enter into a transfer agreement with the overseas recipient based on a "standard contract" to be published by the CAC
    - other mechanisms may be provided in the future

Draft Personal Information Protection Law (Cont'd)

Cross-Border Transfer under Special Circumstances

- **Request for information by foreign judicial or law enforcement organs**
  - Where a foreign judicial or law enforcement organ requests for personal information that is "stored" within China, such personal information shall not be provided unless China's "competent government agency" has approved such a provision.
  - If certain international treaties have relevant provisions, it is allowed to act in accordance with those provisions.
- **"Black List"** of Foreign Entities and Individuals
  - Entities and individuals conducting processing activities "infringing Chinese citizens' rights and interests related to personal information," or "endangering China's national security or public interest"
  - CAC to take measures to restrict or prohibit the cross-border transfer to them
- "**Retaliation**" on Foreign Countries
  - Countries or regions act in a discriminatory or restrictive manner against China with respect to personal information protection
  - China has the right to take "corresponding measures" against such countries or regions

How China Fit Into the Global Picture?

A Conversation on Key Considerations

Question 1: How PIPL is Different From GDPR?

- Example 1: Lawful basis for processing
- Example 2: Processing of publically available information
- Example 3: Personal information subject rights

Divergence from GDPR

- **Lawful basis for processing**
  - Legitimate interest is not a lawful processing basis under the PIPL
  - Processing may be based on consent and other non-consent basis
  - If relying on consent for a processing activity, separate consent is needed under certain circumstances:
    - sharing data with “third parties”
    - public disclosure of personal information
    - processing of sensitive personal information
    - cross-border transfer of personal information

Divergence from GDPR (Cont'd)

- **Processing of publically available information**
  - Consent not needed, if complying with the purpose for which personal information was disclosed.
    - If the original purpose is unclear, process in a reasonable and cautious manner.
  - Obtain separate consent if the processing exceeds the reasonable scope related to the purpose.
  - For processing that has a significant impact on individuals, consent must be obtained.

Divergence from International Practices (Cont'd)

- **Personal information rights:** Largely align with GDPR but lacks precise GDPR language, uncertain whether restrictions or exemptions may apply

GDPR	PIPL	Comments
Right to information	√	The PIPL also states that an individual has the right to request the processing entity to explain their "data processing rules" (e.g. the type(s) of personal information collected, the legal basis relied on, etc.). This is likely covered by the right to information and right to access under the GDPR.
Right to access	√	
Right to correction/rectification	√	
Right to erasure	√	
Right to object to and restrict the processing of an individual's data	√	
Right to data portability	Not available	
Right not to be subject to automated decision-making	√	
Right to withdraw consent	√	
Right to lodge a complaint with a regulator	√	

Question 2: How Multinationals Should Consider their Cross-border Data Transfer Strategies for China?

- **Personal Information**
  - Potential data localization requirements for specific data or category of operators
    - Critical Information Infrastructure
    - Entities processing a large volume of personal information
    - Sectoral data localization requirements (e.g. finance, healthcare)
  - Security assessment process is unclear at the moment
  - Potential liabilities if the overseas recipients fails to protect the personal information, for example, data breach occurred outside of China compromised Chinese data
- **Important Data**
  - Unclear scope of important data
  - Transfer rules pending published by CAC
  - Potential liabilities if the overseas recipients fails to protect the data

Question 3: How to Operationalize the CSL/PIPL/DSL?

- **Examples of Organizational Measures**
  - Appoint a "DPO" if the volume of personal information processed by an entity meet the threshold to be determined by CAC.
  - Implement access management and provide training on a regular basis.
  - Develop and implement an incident response plan.
- **Multi-Level Protection Scheme**
  - Adopt corresponding technical measures and other necessary measures to safeguard data security base on the MLPS
- **"Risk assessment" (DPIA?)**
  - Carry out risk assessment if required (e.g. cross-border data transfer, process personal information through automated methods).
  - Retain the assessment report for at least three years.
- **Leveraging the existing global program**