

China's Data Governance Regime

A Regulatory Reference Case for Digital Infrastructure

Samm Sacks

Senior Fellow, Paul Tsai China Center
Yale Law School

MCDF Digital Infrastructure Workshop Series | March 4, 2026



Yale Law School

WHY STUDY CHINA'S APPROACH

The world's most comprehensive data regime — and its growing pains

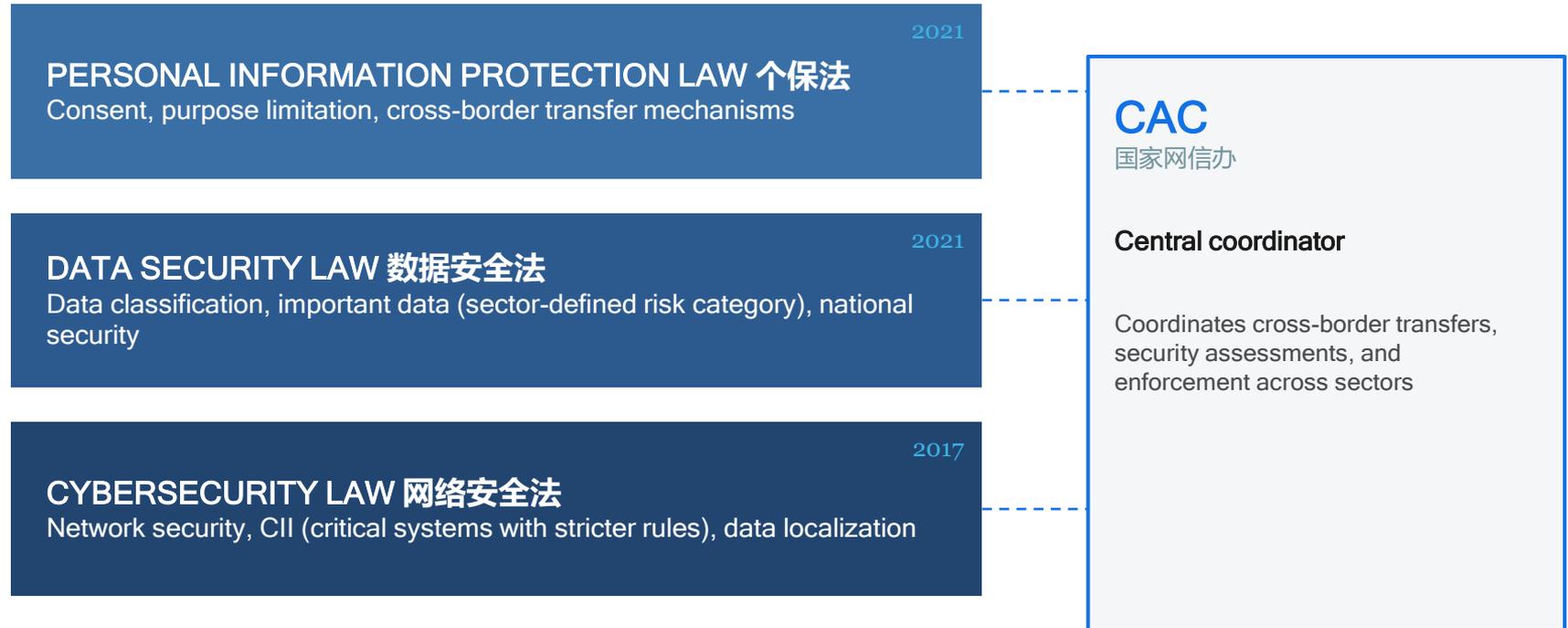
Three laws, dozens of implementing rules, and a hard-learned course correction. China's data regime is a case study in sequencing — what to regulate first, how tightly, and when to ease up.

- **Three foundational laws (2017-2021)** created one of the world's most comprehensive data governance systems
- **Security-first logic:** data classification, localization requirements, and cross-border transfer controls
- **Course correction (2024-2026):** Beijing eased rules after over-tightening chilled business and investment

The lesson: sequencing and calibration matter as much as the rules themselves

LEGAL ARCHITECTURE

Three laws, one logic: security first, rights second, flexibility emerging



CAC coordinates across all three laws, but sector regulators (MIIT, PBOC, MPS) retain enforcement authority – coordination is the hard part.

DATA CLASSIFICATION

Core / important / general — and a practical safe harbor

CORE DATA

核心数据

Strictest controls

National security, economic lifelines,
major public interest

Outbound transfer highly restricted, if
not virtually prohibited

IMPORTANT DATA

重要数据

Sector-defined risk category

Sector-specific catalogues (energy,
transport, finance, health)

Outbound: mandatory security
assessment

GENERAL DATA

一般数据

Standard compliance

Routine business and operational data

Outbound: SCC (standard contract),
certification, or exempt

Safe harbor: No published catalogue → no export-assessment reporting obligation

CROSS-BORDER TRANSFERS

From restrictive to calibrated: the 2022–2026 correction arc



WHAT WENT WRONG, WHAT WORKED

Enforcement, CII risks, and the over-tightening lesson

CII designation can change mid-project

A system designated ordinary today can later become critical infrastructure (CII) – triggering new localization and audit obligations going forward. High stakes for 20-30 year concessions.

Enforcement has teeth

Regulators have pursued high-profile cases against platforms and foreign brands for personal information (PI) misuse. The 2025 CSL amendments introduced harsher, tiered penalties.

The correction worked – but took two years

The 2022 rules over-tightened, chilling routine transfers. The 2024 Provisions recalibrated. Lesson: build flexibility into the architecture from the start.

DIAGNOSTIC QUESTIONS

For your next project review — or your next regulatory draft

CHINA-TOUCHPOINT SCREEN

Is any part of the system hosted or operated in China, or processing personal information of people located in China?

If yes → deeper China-specific due diligence needed

For regulatory design:

How will you classify data without chilling investment?

What transfer mechanisms balance security with viability?

How do you build enforcement credibility without over-tightening?

DESIGN LESSONS FOR ANY DATA REGIME

- 1 What data types will the project generate — and would any qualify as “sensitive” or “important” under host-country rules?
- 2 Will data cross borders? Which jurisdictions’ transfer rules apply?
- 3 Could this asset later be designated “critical” — triggering stricter rules mid-project?
- 4 Do contracts allocate data governance responsibilities — and has anyone mapped what data exists?

