TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT "IT-Sicherheitsrechtstag 2020"

Berlin, 24.09.2020

Das IT-Sicherheitsgesetz 2.0 vor dem Hintergrund der aktuellen chinesischen Cyber Policy

Dr. Dennis-Kenji Kipker, Universität Bremen

China und Cyber = Anlass für Ärger?

NETZAUSBAU

„Menschenrechtsfrage“: Washington erhöht bei der 5G-Entscheidung den Druck auf Berlin

Immer mehr EU-Länder schließen den chinesischen Anbieter Huawei vom 5G-Netz aus. Jetzt redet die US-Regierung der zögerlichen Bundesrepublik ins Gewissen.

Moritz Koch

16.08.2020 - 19:10 Uhr • 9 x geteilt

WELT+ CHINESISCHE APP

Warum Trump TikTok verbieten will

Stand: 14:16 Uhr | Lesedauer: 11 Minuten

Von **Christina Brause**, Maximilian Kalkhof

0

IT-SiG 2.0 und China: Wesentliche Schnittpunkte

- **§ 8a Abs. 3 S. 4 BSIG-E:** Übermittlung einer Liste aller IT-Produkte mit Bedeutung für die Funktionsfähigkeit der Kritischen Infrastruktur an das BSI

- **§ 9a BSIG-E:** Nationales freiwilliges IT-Sicherheitskennzeichen für Hersteller von IT-Produkten

- **§ 9b Abs. 2 BSIG-E:** Pflicht des Betreibers einer Kritischen Infrastruktur, „kritische“ Komponenten beim BMI anzuzeigen und eine Garantieerklärung des Herstellers einzuholen, die sich auf die gesamte Lieferkette des Produktes beziehen muss („Vertrauenswürdigkeitserklärung“)

Chinesische Technologiedominanz = Anlass zur Sorge?

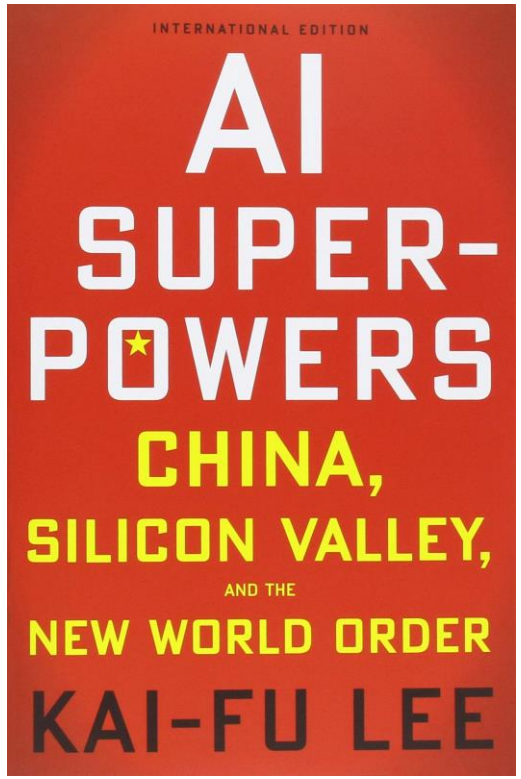
- Aktuelle (globale) politische Entwicklung scheint vor allem eines widerzuspiegeln: zunehmende chinesische Technologiedominanz, die im Ausland entweder auf politische Sorge oder Ablehnung stößt!
- Was ist dran – und viel wichtiger noch – befinden wir uns auf dem richtigen Weg in Sachen nationaler Cybersecurity-Gesetzgebung?
- **→ Beispiel Schlüsseltechnologie KI und IT-Sicherheit: Entwicklung, politische Strategie und aktuelle Rechtsetzung in China**

Herausforderungen der Cybersecurity-Gesetzgebung in China

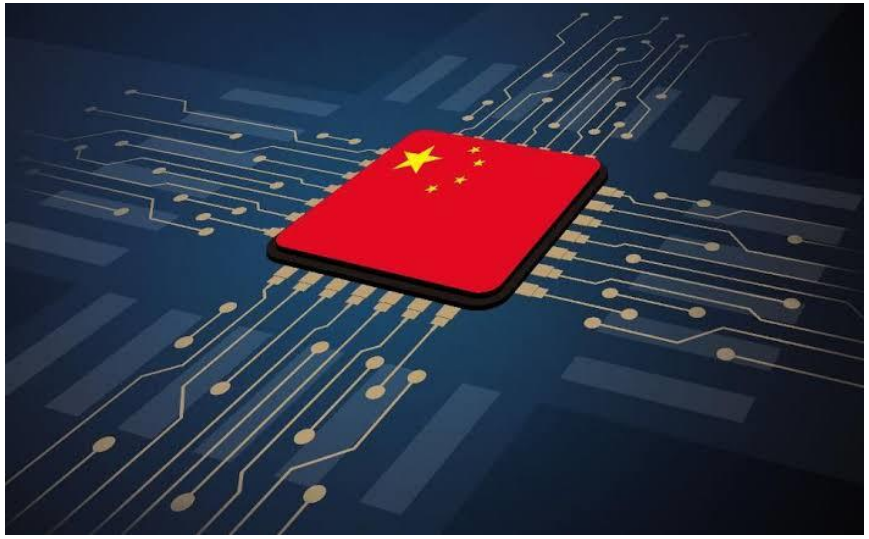
- Seit Jahrzehnten **vielschichtige IT-Sicherheitsgesetzgebung in China**, globale Vorreiterstellung wird zunehmend ausgebaut
- Erstes IT-sicherheitsrelevantes Gesetz: „Computer Information System Security Protection Regulations of the People's Republic of China" **(1994)**
- Geraume Zeit erfolgte chinesische IT-Gesetzgebung nahezu völlig losgelöst vom Westen, ist in den letzten Jahren aber auch hier **immer stärker in den Fokus** der öffentlichen Wahrnehmung gelangt
- **Mögliche Gründe:**
  - Chinesische Unternehmen expandieren zunehmend in Richtung EU
  - Europäische Unternehmen haben mehr und mehr Geschäftskontakte nach China/Auslandsniederlassungen in China
  - Industrie- und staatliche Spionagetätigkeit
- **Erschwerend tritt hinzu:** Unübersichtliche Behörden- und Zuständigkeitsstruktur, mehrere Verwaltungsebenen, generalklauselartige Gesetze, Verschränkung mit technischen Standards

Thema KI: Chinesisches Politikum, das auch uns betrifft!

- **Außerordentliche Relevanz** von KI in politischen Strategien Chinas
- Staatsrat: Volksrepublik soll bis 2025 die **weltweite Führungsposition bei KI** übernehmen
- 2030: **Weltweite Vormachtstellung** in Sachen KI – politisch und wirtschaftlich!
- „Next Generation Artificial Intelligence Development Plan“ **(AIDP, 2017)**: KI wird definiert als zentrale Maßnahme zur Förderung der nationalen, wirtschaftlichen und sozialen Sicherheit von China
- **KI-Gesetzgebung:** kein eigenständiges chinesisches KI-Gesetz, jedoch verschiedene Einzelvorschriften mit Regulierung technisch-organisatorischer Einsatzszenarien, die einen Bezug zur IT-Sicherheit entfalten
- KI-Sicherheit vornehmlich bisher nicht als Aufgabe der **„Security“**, sondern **„Safety“** verstanden
- **→ IT-Sicherheit in der KI-Gesetzgebung in China damit weitläufiges Thema!**



Cybersecurity: Aktuelle Entwicklungen in der chinesischen Gesetzgebung



- Chinese Cybersecurity Law (CSL, 2016)
- Chinese Cryptography Law (2019)
- Chinese Data Security Law (DSL, Entwurf 2020)
- Personal Information Protection Law (Gesetzgebungsverfahren)
- → **Viele Gesetze, ein Hintergrund:** Chinesische Rechtsgrundlagen zur IT- und Datensicherheit sollten stets im Zusammenhang betrachtet werden, da sich die Regulierungsbereiche von einzelnen Gesetzen durchaus überschneiden können!

Chinese Cybersecurity Law (CSL, 2016)

- 2016 verabschiedet, 2017 in Kraft getreten
- Adressiert **IT-Sicherheit und Datenschutz** gleichermaßen – eines der ersten Gesetze Chinas, das explizit datenschutzrechtliche Anforderungen enthält
- Hierzulande viel diskutiert, **breite öffentliche Wahrnehmung**: Regulierung von VPN-Verbindungen, Produktzulassung und Datenlokalisierung
- **(Politische) Hauptziele des CSL:**
  - Sicherstellung der Netzwerksicherheit (= IT-Sicherheit)
  - Aufrechterhaltung der chinesischen Souveränität im Cyberspace
  - Schutz der nationalen Sicherheit und des öffentlichen Interesses Chinas
  - Schutz der Rechte und Interessen von Bürgern, Rechtspersonen und sonstigen Einrichtungen
  - Förderung der wirtschaftlichen und sozialen Entwicklung der chinesischen Gesellschaft

Chinese Cybersecurity Law (CSL, 2016)

Cybersecurity: Vor allem relevant im Hinblick auf Kapitel 2 „Support and Promotion of Network Security“, Kapitel 3 „Network Operations Security“ und Kapitel 5 „Monitoring, Early Warnings, and Emergency Responses“ – mit mittelbarem KI-Bezug:

- **Art. 5:** Der Staat hat die Aufgabe, IT-Sicherheitsrisiken zu überwachen und ihnen vorzubeugen, und die Sicherheit und Ordnung im Cyberspace zu gewährleisten
- **Art. 7:** Der Staat beteiligt sich an internationalem Austausch und Kooperation in der Entwicklung und Nutzung von Netzwerktechnologien
- **Art. 10:** Es sind Maßnahmen vorzuhalten, die die Netzwerksicherheit und operationelle Stabilität des Netzwerks gewährleisten

Chinese Cybersecurity Law (CSL, 2016)

- **Art. 15:** Der Staat begründet, unterhält und verbessert ein System von Netzwerksicherheitsstandards
- **Art. 18:** Der Staat fördert die Entwicklung von IT-Sicherheitstechnologien, und unterstützt innovative Maßnahmen zur Netzwerksicherheit
- **Art. 21:** Ein System der Netzwerksicherheit ist zu etablieren, das entsprechende technische Maßnahmen zum Schutz vor Computerviren, Netzwerkangriffen, und sonstigen schädlichen Eingriffen enthält
- **Art. 51:** Der Staat richtet Systeme zur Netzwerküberwachung ein, sowie zu Frühwarnungen

Chinese Cybersecurity Law (CSL, 2016)

- Überdies: Verschiedene **untergesetzliche Regelwerke** und **technische Normen und Standards** auf Grundlage des CSL als Einfallstor für KI und IT-Sicherheit
- Vielfältige weitere Anwendungsfelder für KI und IT-Sicherheit in China werden identifiziert:
  - Machine Learning
  - Knowledge Graphs
  - Natural Language Processing
  - Human-Computer Interaction
  - Computer Vision
  - Biometric Feature Recognition
  - Virtual Reality (VR)/Augmented Reality (AR)
- → **Einschätzung:** Chinesische KI-Entwicklung geht zukünftig nicht von bereichsspezifischen, sondern von allgemeinen Anwendungsfeldern aus, die eine Vielfalt möglicher Einsatzszenarien abdecken, sodass hiervon zwangsläufig auch die IT-Sicherheit umfasst ist

Chinese Cryptography Law (2019)

- Verabschiedet im Oktober 2019, **Inkrafttreten zum 1.1.2020**
- **Gesetzgeberisches Ziel:** Entwicklung neuer kryptografischer Verfahren, Dienste und Produkte in China → „mittelbar“ dadurch auch Stärkung der IT-Sicherheit (Art. 1)
- **IT-Sicherheit:** Wesentlicher Fokus der öffentlichen und nationalen chinesischen Sicherheitsinteressen → deutliche Parallelen zum CSL
- Generalklauselartige Formulierungen, kein Ausschluss von **KI als Technologieträger**
- **Flexibilität und Anpassungsoffenheit** als neue Schlüsselelemente chinesischer Kryptografiegesetzgebung

Chinese Cryptography Law (2019)

- **Systematischer Aufbau:**
  - Kapitel 1: General Provisions
  - Kapitel 2: Core Cryptography, Common Cryptography
  - Kapitel 3: Commercial Cryptography
  - Kapitel 4: Legal Responsibility
  - Kapitel 5: Supplementary Provisions
- **Regulierungsschwerpunkt:** Unterscheidung zwischen den unterschiedlichen kryptografischen Verfahren mit gestuften, unterschiedlichen Nutzungsanforderungen
  - **Core und Common Cryptography:** Einsatz zum Schutz von Staatsgeheimnissen = selbst Einstufung als Staatsgeheimnis
  - **Commercial Cryptography:** Einsatz zum Schutz jeglicher Information, die kein Staatsgeheimnis ist – somit für sämtliche „herkömmlichen“ Daten → IT-Sicherheit von Unternehmen + Privatpersonen
- **Risikosphäre:** Entwicklung und Anwendung kryptografischer Verfahren erfordert Schutz vor Kompromittierung (vgl. Art. 17, 24)

Chinese Data Security Law (DSL, Entwurf 2020)

- **Bedarf für ein weiteres Gesetz mit einem Bezug zur IT-Sicherheit?**
- **Anfang Juli 2020:** Veröffentlichung des Entwurfs für ein neues chinesisches Datensicherheitsgesetz (Data Security Law, DSL) vom Standing Committee of the National People's Congress (NPC)
- Öffentliche Kommentierungsphase endete am **16. August 2020** → frühe erste Entwurfsfassung, mit Änderungen zu rechnen
- **Systematik:** Gleichrangige Regelung neben CSL
- **Regelungszweck:** adressiert nicht nur IT- und Datensicherheit, sondern primär den Umgang mit Daten als Wirtschaftsgut, die Modalitäten von Datenverarbeitungsvorgängen, die Regelung von Zugriffsmöglichkeiten, und Möglichkeiten zu Open Data
- **Relevante Abschnitte:** Kapitel 2 („Data Security and Development"), Kapitel 3 („Data Security Systems"), Kapitel 4 („Data Security Protection Responsibilities"), Kapitel 5 („Government Data Security and Openness")

Chinese Data Security Law (DSL, Entwurf 2020)

Wichtige Einzelvorschriften mit KI- und IT-Sicherheitsbezug:

- **Art. 12:** Der Staat ergreift Maßnahmen, um einerseits die Datensicherheit zu befördern, andererseits aber auch die Datennutzung zu ermöglichen
- **Art. 13:** Der Staat verabschiedet eine Big Data-Strategie. Zur Datennutzung sind innovative Technologien notwendig, wie sichere KI-gestützte Methoden der Datenauswertung
- **Art. 14:** Der Staat fördert die wissenschaftliche Forschung im Bereich der Datenentwicklung und Datennutzung
- **Art. 19 ff.:** Unterteilung von Datenbeständen in unterschiedliche Schutzklassen, jeweils in Abhängigkeit der Bedeutung für die wirtschaftliche und soziale Entwicklung, und gemessen an den Auswirkungen auf die nationale Sicherheit, das öffentliche Interesse und die Rechtsordnung
- **Art. 20:** Zentralisiertes System der Risikoüberwachung inkl. Frühwarnsystem, KI-gestütztes Monitoring möglich

Chinese Data Security Law (DSL, Entwurf 2020)

Wichtige Einzelvorschriften mit KI- und IT-Sicherheitsbezug:

- **Art. 25:** Für die Datenverarbeitung Verantwortliche müssen ein compliancekonformes Management zur Datensicherheit etablieren, das sich auf den gesamten Arbeitsablauf der Organisation erstreckt
- **Art. 27:** Soweit Daten verarbeitet werden, sollte eine Risikoüberwachung etabliert werden, die auch die IT- bzw. Datensicherheit betrifft. Eine solche Risikoüberwachung kann KI-gesteuert erfolgen
- **Art. 36:** Staatliche Einrichtungen, die Daten verarbeiten, müssen ein Management zur Datensicherheit implementieren, die Auslagerung an Dritte hat keine Entbindung von der primären Verantwortlichkeit zur Folge. Die Einhaltung von TOM ist zu überwachen
- **Art. 41:** IT-und Datensicherheit ist in einem fortlaufenden Prozess sicherzustellen – dies gilt sowohl für Aufsichtsbehörden als auch für datenverarbeitende Stellen

IT-SiG 2.0 im chinesischen Kontext: Quo vadis?

- Chinesische Schlüsseltechnologien (hier am Beispiel KI) unterliegen einer **umfassenden Regulierung**
- **Der Blick in das Gesetz macht deutlich: Wirtschaftsschutz** ein Gesichtspunkt, aber Verfolgung und Schutz von **staatlichen Interessen** steht doch im Mittelpunkt
- Am Beispiel KI wird überdies klar: China will die **politische und wirtschaftliche Vorherrschaft im digitalen Raum** sichern, und ist bereits auf dem Weg dahin
- Mit Blick auf nationale Regulierungsvorschläge zum IT-SiG 2.0: **„Misstrauen" erst einmal durchaus berechtigt**, denn auch hier geht es um den Schutz von Schlüsseltechnologien!
- **Entscheidende Frage aber auch hier wieder:** Sind wir auf dem richtigen Weg? Für wen entstehen hier die Mehrbelastungen – i.e.L. nämlich auch für die Betreiber als „Leidtragende"!
- **→ Deshalb kann der gegenwärtige Entwurf des IT-SiG 2.0 (Stand Mai 2020) definitiv noch nicht das letzte Wort sein, das hier gesprochen wurde!**

Vielen Dank für Ihre Aufmerksamkeit – ich freue mich auf die Diskussion!

Dr. Dennis-Kenji Kipker

dennis.kipker@certavo.de

+49 421 21866049