Chinese Cybersecurity Law:
Neue rechtliche Wege und Umwege nach China

Dr. Dennis-Kenji Kipker

Legal Advisor

CERT@VDE

Bonn, 21.05.2019

DKE

VDE DIN

Hiobsbotschaften aus Fernost – oder Panikmache aus Deutschland?

Handelsblatt

HOME POLITIK UNTERNEHMEN FINANZEN TECHNIK AUTO KARRIERE ARTS & STYLE MEINUNG VIDEO SERVICE

Deutschland Konjunktur International Konjunkturdaten Ökonomische Bildung Weltgeschichten

Handelsblatt > Politik > International > Digitalisierung: Das zweite Gesicht Chinas

Suchbegriff, Wi

DIGITALISIERUNG

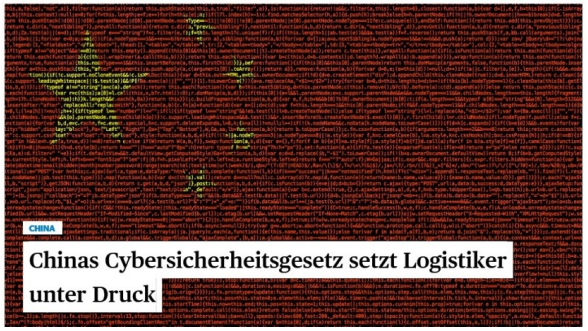
Das zweite Gesicht Chinas

DVZ Deutsche Verkehrs-Zeitung

Abo Shop Werbung Newsletter Veranstaltungen Print Jobs Sofort-Zugang Login

LAND SEE LUFT LOGISTIK POLITIK MENSCHEN MEINUNG MEHR Suchbegriff eingeben...

Startseite > Region > Länder > China > Chinas Cybersicherheitsgesetz setzt Logistiker unter Druck



CHINA

Chinas Cybersicherheitsgesetz setzt Logistiker unter Druck

German firms hit by China's internet crackdown

Beijing has scaled up internet censorship, disrupting German corporate operations in China and heightening fears of state-sponsored espionage.

Dana Heide Jean-Michel Hauteville

02/01/2018 - 04:41 PM • Share now

China macht das Internet dicht

Die Regierung in Peking blockiert heute die letzten Schleichwege ins freie Internet. Das trifft auch westliche Firmen.

tcafés. Foto: Jie

Historiker
erden, an dem China
zeit der
dieses Wochenende

Artikel zum Thema

China zensiert Whatsapp vor Parteitag der Kommunisten

DKE
VDE DIN

Inhalte

- Systematik des chinesischen Cybersicherheitsrechts
- Aufbau und Regelungsziele des CSL
- Zentraler Begriff des „Network operators“
- Critical Information Infrastructure (CII)
- Abgestuftes Cyber-Sicherheitssystem
- Personal Information Security (PIS)
- Cross Border Data Transfer
- VPN-Regulierung
- Zertifizierung und Produktzulassung
- Kryptografie
- Fazit und Ausblick

Systematik des chinesischen Cybersicherheitsrechts I

- **Chinese Cybersecurity Law (CSL)** aus 2016, Inkrafttreten Juni 2017
- **Doch nicht nur ein Gesetz zur Cybersicherheit in China**, so z.B.:
  - Computer Information System Security Protection Regulations of the People's Republic of China (1994)
  - Administrative Provisions on Computer Information System Security Specialized Testing and Sales Licenses (1997)
  - Computer Virus Prevention and Management Measures (2000)
  - Telecommunications Regulations of the People's Republic of China (Novelle von 2016)
  - Cryptography Law of the People's Republic of China (Entwurf, April 2017)

Systematik des chinesischen Cybersicherheitsrechts II

- **Charakteristik:**
  - Chinesische Gesetzgebung eher als **allgemeiner „Rechtsrahmen“** zu verstehen
    - Politische Strategie, Weißbuch
  - Stärkere **Verschränkung von Recht und Technik** als z.B. in Deutschland
  - **Konkretisierung** vielfach durch technische Normen und Standards und untergesetzliche Regelungen
    - **Normung:** Federführend Chinesisches Nationales Normungskomitee zur technischen Standardisierung der Informationstechnologie (TC 260), untersteht unmittelbar der Chinesischen Cybersicherheitsbehörde CAC
    - **Untergesetzliche Regelungen:** Z.B. September 2018 „Regulations for Internet Security Supervision and Inspection by Public Security Organs“ des Ministry of Public Security (MPS), enthält technische Implementierungs- und Prüfpflichten für das CSL

Chinese Cybersecurity Law: Aufbau und Regelungsziele

- **Doppelter Fokus:**
  - Netzwerksicherheit
  - Datenschutz
  - Vergleich mit EU: DS-GVO und NIS-RL, Cybersecurity Act
- **Netzwerksicherheit:** Chinesische Netzwerke sollten sich in einem stabilen und verlässlichen Arbeitszustand befinden, es sollten Maßnahmen (TOM) gegen Einbrüche, Zerstörung oder gegen den rechtswidrigen Einsatz von Netzwerkressourcen ergriffen werden
- **Datenschutz:** Schutz personenbezogener Daten, die die Identifizierung von Personen ermöglichen
  - Einwilligung, Datensparsamkeit, Privacy by Design, TOM, Vertraulichkeit, Zweckbindung, Einwilligungserklärung für die Nutzung von Daten, Regulierung von Datenschutzverletzungen, Betroffenenrechte, Verarbeitungsverzeichnis

Chinese Cybersecurity Law:
Zentraler Begriff des „Network operators“

“Any entity with a network of computers (three or more) is considered a network operator.”

- CAC -

“Effectively, all businesses and organisations operating in China can be considered as network operators.”

Chinese Cybersecurity Law:
Critical Information Infrastructure (CII) I

- CSL enthält in Kap. 3, Abschnitt 2 **einen eigenständigen Abschnitt zum Schutz von kritischen Informationsinfrastrukturen** (Art. 31 ff.)
- **Definition von CII gem. CSL nicht abschließend:** öffentliche Kommunikations- und Informationsdienste, Energieversorgung, Verkehr, Wasserversorgung, Finanzen, öffentliche (Verwaltungs)dienste, eGovernance und weitere
  - **Kriterium:** Zerstörung, Funktions- oder Datenverlust gefährdet in schwerwiegendem Maße die nationale Sicherheit, den nationalen Wohlstand, das öffentliche Wohl
- **Erweiterte Cybersecurity-Pflichten für CII-Anbieter,** u.a. National Security Review für eingesetzte IT-Produkte, Pflicht zur Datenlokalisierung für Personal Information (PI)
- CSL wirkt sich faktisch somit auch auf ausländische (deutsche) Hersteller und Anbieter aus
- **Problem:** Welche Einrichtungen konkret betroffen sind, wird durch das CSL nicht bestimmt
  - Klarstellung durch **„Critical Information Infrastructure Protection Regulations“** erwartet (zzT. Entwurfsfassung aus Juni 2017)

Chinese Cybersecurity Law:
Critical Information Infrastructure (CII) II

- **Aktuelle, im Bereich CII relevante chinesische Standards:**
  - Cyber Security Protection Requirements of Critical Information Infrastructure (Entwurf)
  - Guide to Security Inspection and Evaluation of Critical Information Infrastructure (Entwurf, August 2018)
  - Security Controls of Critical Information Infrastructure (Entwurf, Juni 2018)
  - Indicator System of Critical Information Infrastructure Security Assurance (Entwurf, August 2018)
- **Weitere Standards in Planung,** insb. auch zur Identifikation von CII, Verabschiedungszeitpunkt zzT. jedoch noch unklar

Chinese Cybersecurity Law:
Abgestuftes Cyber-Sicherheitssystem I

- Artt. 21, 31 CSL schreiben die **Implementierung eines abgestuften („tiered“) Cyber-Sicherheitssystems** vor, das mit technisch-organisatorischen IT-Sicherheitspflichten einhergeht, explizit angesprochen sind auch CII
- **Konkretisierendes Dokument:** Regulation on Classified Cyber Security Protection des MPS
  - Anwendbar auf alle Netzwerkbetreiber
  - Bewertung und Klassifizierung der Systeme von Level 1-5 (niedrig-hoch) in Abhängigkeit der gefährdeten Rechtsgüter und der bei ihnen eintretenden Schadenshöhe
  - Spezifische IT-Sicherheitsstandards für jede Risikogruppe
- **Einschätzung:** Großteil der Unternehmen/Organisationen unterfällt den Risikogruppen 1-2
- **Level 3 z.B.:** Energieversorger, Cloudprovider, etc. → Ab Level 3 Einstufung zugleich als CII möglich

Chinese Cybersecurity Law:
Abgestuftes Cyber-Sicherheitssystem II

- **Ab Level 3: Höhere IT-Sicherheits-Managementanforderungen, z.B.:**
  - Notfallmanagement
  - Hintergrundüberprüfung der Mitarbeiter
  - Durchführung der technischen Wartung in China
  - Netzwerkverschlüsselung
  - Sicherheitsüberprüfungen durch chinesische Stellen, die durch die State Cryptography Administration akkreditiert wurden, z.B. das Shanghai Information Security Testing Evaluation and Certification Center (eine vollständige Liste solcher Stellen existiert zzT. jedoch nicht)
- **Für das abgestufte Sicherheitssystem relevante Standards:**
  - Guidelines for Grading of Classified Cyber Security Protection (Entwurf, August 2018)
  - Implementation Guide for Cyber Security Classified Protection (Entwurf, Dezember 2016)

Chinese Cybersecurity Law: Personal Information Security (PIS) I

- **Datenschutz neben Cybersicherheit Hauptaspekt** der Regulierung durch CSL, da “Data Breaches” in China in der Vergangenheit an der Tagesordnung gewesen sind
- Datenschutz wird im CSL deshalb im Rahmen eines eigenen Kapitels reguliert: **“Chapter IV: Network Information Security”**
- **Einschlägiger Standard:** Personal Information Security Specification (Entwurf, Januar 2019) enthält detaillierte Vorgaben zur Datenverarbeitung von Netzwerkbetreibern
- Grds. Wird die **Einwilligung** zur Erhebung personenbezogener Daten vorgeschrieben, für sensitive Daten gilt das Erfordernis “expliziter Einwilligung”
- Unterscheidung zwischen **“Basic Business Functions”** und **“Extended Business Functions”** und den damit jeweils verbundenen rechtlichen Anforderungen zur DV
- **Konkretisierung des Personal Information Security Incident Reporting System** gem. Art. 42 CSL
- Auch ansonsten: Übernahme zahlreicher Regelungsprinzipien aus der **EU DS-GVO**

Chinese Cybersecurity Law:
Personal Information Security (PIS) II

- **Pflicht zur Bestellung eines DPO**, falls der Netzwerkbetreiber:
  - Personenbezogene Daten von mehr als 500.000 Personen verarbeitet oder
  - Mehr als 200 Personen beschäftigt, die mit der Datenverarbeitung befasst sind
- Pflicht von Netzwerkbetreibern zur **jährlichen Risikoanalyse** (Wahrscheinlichkeit und Folgen einer Datenschutzverletzung)
  - Datenverarbeitungen mit einem **hohen Risikolevel** können ausgeschlossen werden
- **Weiterer Standard zur PIS:** Guidelines for Personal Information De-identification (Entwurf, August 2017)

Chinese Cybersecurity Law: Cross Border Data Transfer I

- Laut CAC entstehen gem. Art. 31 CSL im grenzüberschreitenden Datenverkehr **nicht nur Pflichten für CII, sondern für alle Netzwerkbetreiber**, die personenbezogene und wichtige Daten verarbeiten
  - Definition „wichtiger Daten“: Daten, die einen engen Bezug zur nationalen Sicherheit, wirtschaftlichen Entwicklung, sozialen und öffentlichen Interessen aufweisen
  - Personenbezogene Daten: Zunächst wohl Grenze von 500.000 Personen, nun nicht mehr genannt
- Hierunter fällt insb. eine Überprüfung von Datenströmen, bevor diese die VR China verlassen **(de-facto Datenlokalisierung)**, konkretisierende Dokumente:
  - Measures for Security Assessment of the Cross-Border Transfer of Personal Information and Important Data (Entwurf, April 2017)
  - Guidelines for Data Cross-Border Transfer Security Assessment (Entwurf, Januar 2018), enthält zudem einen Anhang mit der Spezifikation “wichtiger Daten” für 27 Sektoren, u.a. TK, Ernährung, Pharmazie, Finanzwesen, E-Commerce

Chinese Cybersecurity Law:
Cross Border Data Transfer II

- **Zulässigkeit einer Auslandsdatenübermittlung richtet sich nach vorangegangener Risikobeurteilung:**
  - Kriterien u.a.: Folgen eines Datenverlusts, Ausgleichsmaßnahmen zur Datensicherheit
  - Bewertung resultiert in einem Risikoindex der Klassen „niedrig“, „hoch“ und „sehr hoch“
  - Daten der letztgenannten Risikoklassen sind in Mainland China zu speichern
- **Vorfälle in Bezug auf die personenbezogenen und wichtigen Daten** sind den zuständigen Aufsichtsbehörden mitzuteilen; der Datentransfer ist zu unterbrechen
- Auslandsdatenübermittler sollten **Vertraulichkeitsvereinbarungen** mit den Datenempfängern abschließen

Chinese Cybersecurity Law: VPN-Regulierung I

- **Keine expliziten gesetzlichen Vorgaben** zur Regulierung von VPN im CSL
- Regulierungsansatz daher über **Generalklauseln** denkbar:
  - **Art. 5** (staatliche Maßnahmen zum Umgang mit Netzwerksicherheitsrisiken im In- und Ausland; Bekämpfung gesetzeswidrigen Cyberverhaltens)
  - **Art. 58** (zeitweilige Maßnahmen/Beschränkungen der Netzwerkkommunikation in bestimmten Regionen aus wichtigen öffentlichen Interessen)
- **Stand Januar 2019:** Bisher keine einschlägigen Erfahrungswerte kommuniziert, dass VPN-Verbindungen in signifikant größerem Umfang als bisher blockiert wurden bzw. sich die Zahl von Verbindungsproblemen signifikant erhöht hat

Chinese Cybersecurity Law: VPN-Regulierung II

- **Ausblick:**
  - **31. März 2019:** Ablauf der nächsten von chinesischer Seite angekündigten „Deadline“
  - **Weiterentwicklung chinesisch-staatlich lizensierter VPNs:** Ankündigung von MIIT zur Verpflichtung der TK-Diensteanbieter, keine Nutzung von ungenehmigten VPNs zu ermöglichen
  - Vermutung, dass **neues chinesisches Kryptografiegesetz** erhebliche Auswirkungen auf den transnationalen Datentransfer haben wird

Chinese Cybersecurity Law: Zertifizierung und Produktzulassung I

- **Behördliche Überprüfung** von „kritischer Netzwerkausrüstung“ und „spezifischen Cybersicherheitsprodukten“ mit sensiblen Einsatzzwecken (insb. CII), bevor diese auf dem chinesischen Markt vertrieben werden können
- **Rechtsgrundlage:** Art. 23 CSL
- **Betroffenheit:** Richtet sich nach Produktkatalog aus Juni 2017, der durch die Cyberspace Administration of China (CAC), das Ministry of Industry and Information Technology (MIIT), das Ministry of Public Security (MPS) und durch die Certification and Accreditation Administration of China (CNCA) publiziert wurde
  - Produktkatalog unterliegt **laufender Überarbeitung**
- **Betroffene Produkte:** U.a. Router, Switches, Server, Firewalls, Anti-Spam-Produkte, alle ab einer festgelegten Leistungsgrenze

Chinese Cybersecurity Law: Zertifizierung und Produktzulassung II

- **Standards:** Erarbeitung durch das technische Normungskomitee für Informationssicherheit (TC 260, CAC)
  - Berücksichtigung auch von internationalen IT-Standards in ggf. abgewandelter Form
- **Produktprüfung** abhängig von Antragstellung bei jeweils zuständiger akkreditierter Stelle
- **Zahlreiche akkreditierte Stellen und Prüflabore** sowohl staatlich als auch privatrechtlich für unterschiedliche Branchen und Sachbereiche (jedoch keine ausländischen Organisationen)
- **Überprüfte Inhalte:** Schwerpunkt v.a. auf „information security robustness and quality assurance”
- **Vorgehen:** Zunächst zufallsgesteuerte Qualitätskontrollen des Produkts, anschließend Überprüfung der Produktions- bzw. Entwicklungsstätte; Maßstab sind wohl i.e.L. inländische Standards
- **Weitergabe der Prüfergebnisse:** Diese werden an MIIT, CNCA und MPS übermittelt

Chinese Cybersecurity Law: Kryptografie

- Kryptografie **weiteres zentrales Regulierungsthema** im CSL
- ZzT. noch **keine konkretisierenden Standards vorhanden**, Schaffung entsprechender Vorgaben hat jedoch hohe politische Priorität
- Entwurf des chinesischen Kryptografiegesetzes (April 2017) inhaltlich ähnlich weit gefasst wie schon CSL 2016
- Daher auch hier inhaltliche Konkretisierung und Ausgestaltung vor allem durch **untergesetzliche Regulierung und Standards** zu erwarten
- **Vorgeschlagene Kerninhalte des Gesetzentwurfs:**
  - Personenbezogene und wichtige Daten sind zu verschlüsseln
  - Unterscheidung zwischen der Verschlüsselung von Daten bei öffentlichen und privaten Stellen
  - TK- und ISPs sollten u.a. Dechiffrierungsunterstützung anbieten
  - In- und Exportregelungen für kommerzielle kryptografische Produkte sowie behördliche Genehmigungen
  - Sicherheitsbewertung von CII und Kryptografieprodukten und -services durch die State Cryptography Administration

Fazit und Ausblick

- CSL als ausländischer Rechtsetzungsakt auch hierzulande (und global) von **hoher und zunehmend weiterer Bedeutung**
- Nicht nur die Sprachbarriere, sondern auch das grds. andere **Verständnis von Rechtsetzung im deutsch-chinesischen Vergleich** erschweren die Zugänglichkeit zum CSL und dessen rechtliche Systematisierung
- Zahlreiche konkretisierende, **untergesetzliche Rechtsvorschriften sowie Standards** zurzeit noch nicht verabschiedet, daher von offizieller chinesischer Seite auch nicht immer klare inhaltliche Auskünfte möglich
- Gerade auch die **umfassende außergesetzliche Regulierung** erschwert (nicht nur für KMU!) den Überblick
- **Umfassende weitere Rechtsetzungstätigkeit in China in Aussicht**, u.a. auch angetrieben durch das Chinese Cryptography Law
- Daher **Zugang zum chinesischen Markt** unter Compliance-Gesichtspunkten schon jetzt und auch zukünftig mit **zahlreichen Herausforderungen** verbunden

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Dr. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE
Mail: dennis-kenji.kipker@vde.com
Mobil: 0151 40223163

DKE
VDE DIN