Universität Bremen

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Fachbereich 06
Rechtswissenschaft

Cybergesetze in China – Auswirkungen auf deutsche Unternehmen

1. Kölner Cyber Insurance Forum

Prof. Dr. Dennis-Kenji Kipker

Wenn wir aktuell an VR China denken…

Deutschlandfunk

Datenschutz und Geopolitik

Warum TikTok immer öfter verboten wird

Um die besonders bei jungen Le
Verbotsdebatte entbrannt: Ist si
ball geopolitischer Interessen? I
App kommt aus China.

25.05.2023

FORSCHUNG

Fraunhofer kooperiert mit Huawei – Ampelpolitiker fürchten Spionage

Sollen deutsche Wissenschaftler noch mit chinesischen Unternehmen kooperieren? In dieser Frage gerät die
in den Fokus – und

ZEIT ONLINE

Neuerer

Volt Typhoon

Microsoft meldet chinesische Cyberspionage in den USA

Die Hackergruppe Volt Typhoon soll in den USA kritische Infrastruktur ausspioniert haben. Geheimdienste mehrerer Länder warnen vor ähnlichen Angriffen weltweit.

Aktualisiert am 25. Mai 2023, 12:35 Uhr / Quelle: ZEIT ONLINE, Reuters, AFP, ut / 28 Kommentare /

Wenn VR China aktuell an uns denkt…

Menü TAGESSPIEGEL An

Technik-Fehde zwischen China und den USA Peking warnt vor Chips von US-Hersteller Micron

Im Streit um die Lieferung von Hochtechnologien warnen chinesische Behörden vor Bauteilen d US-Konzerns Micron. Es bestünden bedeutende Sicherheitsrisiken, hieß es.

22.05.2023, 11:09 Uhr

EDITION IN DELHI 27°C THE TIMES OF INDIA

World China US Pakistan South Asia UK Europe Middle East Rest Of World Mad, Mad World Photos Vi

NEWS / WORLD NEWS / CHINA NEWS / China Rejects Claim It Is Spying On Western Critical Infrastructure

TRENDING TOPICS New Zealand Fire : At least six killed in New Zealand hostel fire

China rejects claim it is spying on Western critical infrastructure

Reuters /

CNN BUSINESS Markets Tech Media Calculators Videos

Markets →		
DOW	32,813.26	0.04% ▲
S&P 500	4,157.62	1.03% ▲
NASDAQ	12,716.81	1.86% ▲

Fear & Greed Index → Greed is driving the US market 63

Latest Market N Virgin Galactic la Microsoft leaps i Mortgage rates

China has widened its already sweeping counter-espionage law. Experts say foreign businesses should be worried

By Simone McCarthy and Nectar Gan, CNN
Updated 2:13 AM EDT, Thu April 27, 2023

Die Probleme sind aber keineswegs neu!

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, WKN, ISIN

DIGITALISIERUNG

Das zweite Gesicht Chinas

Auf der Weltbühne predigt Peking freien Handel. Zuhause dreht der Staat ausländischen Unternehmen das freie Internet ab. Gerade kleine Firmen und Mittelständler stellt das vor große Probleme.

Dana Heide Sha Hua

28.01.2018 - 17:37 Uhr • 2 x geteilt

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

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

Herausforderungen der Cybergesetzgebung im Reich der Mitte

- **Seit Jahrzehnten vielschichtige Cybergesetzgebung in China, geprägt v.a. durch protektionistische und wirtschaftliche Interessen**
- **Erstes cyberrelevantes 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 nach wie vor in Richtung EU
  - Europäische Unternehmen haben nach wie vor Geschäftskontakte nach China/Auslandsniederlassungen in China
  - Industrie- und staatliche Spionagetätigkeit
  - Digitale Souveränität und China-Taiwan-Konflikt
- **Erschwerend tritt hinzu: Unübersichtliche Behörden- und Zuständigkeitsstruktur, mehrere Verwaltungsebenen, generalklauselartige Gesetze, Verschränkung mit zahllosen technischen Standards, erhebliche Sanktionen bei Verstößen**

Chinesische Cybergesetze und ihre Auswirkungen auf internationale Unternehmen

- **Regulierung von VPN-Verbindungen:**
  - Übermittlung sensibler Unternehmensdaten: Für transnational operierende (deutsche) Unternehmen von Relevanz
  - Perspektivisch problematisch: Nutzung ausschließlich staatlich-lizensierter VPNs
- **Produktzertifizierung und Produktzulassung:**
  - Strenge Vorgaben für IT-Importe nach China u.a. für Netzwerkausrüstung und Cybersicherheitsprodukte
  - Spezifizierung durch verschiedene chinesische Behörden u.a. Cyberspace Administration of China (CAC)
  - Weit gefasster Produktkatalog betrifft u.a. Router, Switches, Server, Firewalls
- **Datenlokalisierung:**
  - Daten, die beim Betrieb von Kritischen Infrastrukturen anfallen, sind grds. im chinesischen Inland zu speichern
  - Ausgedehnter Pflichtenkreis durch neue chinesische Datenschutzregulatorik (z.B. Betrieb von E-Mail-Postfächern chinesischer Mitarbeiter auf ausländischen Servern)

Zentrale Rechtsquellen chinesischer Cybergesetzgebung

- → **Chinese Cybersecurity Law (CSL, Inkrafttreten zum 1.6.2017)**
- → **Chinese Cryptography Law (Inkrafttreten zum 1.1.2020)**
- → **Chinese Data Security Law (DSL, Inkrafttreten zum 1.9.2021)**
- → **Chinese Personal Information Protection Law (PIPL, Inkrafttreten zum 1.11.2021)**
- → **Chinese Counter Espionage Law (Novelle mit Inkrafttreten zum 1.7.2023)**
- → **Außerdem:** Export Control Law (ECL, Inkrafttreten zum 1.12.2020), Criminal Law, Tort Liability Law, Law on the Protection of Consumer Rights and Interests, Measures for the Management of Scientific Data (SDM, Inkrafttreten zum 17.3.2018), General Provisions of the Civil Law of the People's Republic of China

Zentrale Rechtsquellen chinesischer Cybergesetzgebung

→ **Viele Gesetze, ein Hintergrund: Chinesische Cybergesetze sollten stets im Zusammenhang betrachtet werden, da sich die Regulierungsbereiche von einzelnen Vorschriften durchaus überschneiden können!**

Cybersecurity Law (CSL)

“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.”

Cybersecurity Law (CSL)

- **Adressiert IT-Sicherheit und Datenschutz gleichermaßen – eines der ersten Gesetze Chinas, das explizit datenschutzrechtliche Anforderungen enthält**
- **Hierzulande viel diskutiert, breite öffentliche Wahrnehmung v.a. wegen Regulierung von VPN-Verbindungen**
- **(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

Cybersecurity Law (CSL)

- **Implementierung eines abgestuften („tiered“) Cyber-Sicherheitssystems, 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**

Cybersecurity Law (CSL)

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

Cybersecurity Law (CSL)

- **Personal Information Security (PIS): Datenschutz neben Cybersicherheit Hauptaspekt der Regulierung durch CSL, da “Data Breaches” in VR China in der Vergangenheit an der Tagesordnung gewesen**
- **Übernahme zahlreicher Regelungsprinzipien aus der EU DS-GVO (dazu noch im Folgenden…)**
- **Unterscheidung zwischen “Basic Business Functions” und “Extended Business Functions” und den damit jeweils verbundenen rechtlichen Anforderungen zur Datenverarbeitung**

Cybersecurity Law (CSL)

- **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

Cybersecurity Law (CSL)

- **Cross Border Data Transfer: Laut CAC entstehen im grenzüberschreitenden Datenverkehr nicht nur Pflichten für CII, sondern für alle Netzwerkbetreiber, die personenbezogene und wichtige Daten verarbeiten**
- **Hierunter fällt insb. eine Überprüfung von Datenströmen, bevor diese die VR China verlassen (de-facto Datenlokalisierung)**
- **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
- **Auslandsdatenübermittler sollten Vertraulichkeitsvereinbarungen mit den Datenempfängern abschließen**

Personal Information Protection Law (PIPL)

Allgemeine Faustregel:

Die Datenverarbeitung darf nicht der nationalen Sicherheit oder dem öffentlichen Interesse schaden!

Personal Information Protection Law (PIPL)

- **Gilt für private und staatliche Organe**
- **Extraterritoriale Wirkung insb. bei Bereitstellung von Produkten/Dienstleistungen auf chinesischem Markt und Verhaltensanalyse**
- **Personenbezogenes Datum: Alle Arten von Informationen, die elektronisch/auf anderem Wege aufgezeichnet werden und sich auf identifizierte/identifizierbare natürliche Personen beziehen**
- **Sensibles Datum, Beispiele: biometrische Merkmale, religiöse Überzeugungen, medizinische Gesundheit, Finanzkonten, Standortdaten, Minderjährige unter 14 Jahren**
- **Verarbeitung: u.a. Erhebung, Speicherung, Nutzung, Übermittlung, Bereitstellung, Offenlegung, Löschung**
- **Definition von Datenverarbeitungsgrundsätzen inkl. Datensicherheit und Kopplungsverbot**
- Hohe Sicherheitsanforderungen für Internetplattformen, große Nutzerzahl, komplexe Geschäftsmodelle

Personal Information Protection Law (PIPL)

- **Gesetzlich festgeschriebene Tendenz zur Datenlokalisierung (z.B. für Datenanfragen ausländischer Justiz- und Strafverfolgungsbehörden)**
- **Grenzüberschreitender Datentransfer unterliegt hohen Anforderungen:**
- Staatliche Sicherheitsbewertung
- Staatlich gelenkte Zertifizierung
- Abschluss eines staatlich formulierten „Standardvertrags“
- Benennung eines Vertreters in der VR China
- „Angemessenheitsbeschlüsse“ für den Drittlandtransfer aus VR China möglich
- **Staatliche „Blacklist“ für ausländische Datenverarbeiter, die nationale Sicherheitsinteressen beeinträchtigen**
- **Umfassende behördliche Kontrollbefugnisse und Sanktionsmittel**

Worauf müssen Unternehmen sich einstellen und was ist ihnen zu raten?

- **Faktische und rechtliche Auswirkungen chinesischer Cybergesetze auf nationale Unternehmen sind schon jetzt enorm**
- **Trotz teils ähnlicher/vergleichbarer Anforderungen z.B. für TOM in der Datensicherheit und Datenschutzgrundsätze oftmals gänzlich andere „Stoßrichtung“**
- **Generalklauselartige Anforderungen, komplexe Zuständigkeitsstruktur und strenge Weisungsabhängigkeit der Behörden (z.B. keine unabhängige Datenschutzaufsicht) erschweren Interessenwahrnehmung**
- **Zugang zum chinesischen Markt jetzt und in Zukunft mit erheblichen Herausforderungen und Kosten für Compliance-Konformität verbunden (vgl. z.B. Ausweitung Anwendungsbereich Chinese Counter Espionage Law)**
- **<u>Empfehlung:</u> Kein ungeregelter Marktzugang, umfassendes Risk Assessment vorab, Identifikation regulatorischer Anknüpfungspunkte, vorab Aufbau eines vertrauenswürdigen nationalen Kontakts/Anlaufstelle**

Universität Bremen

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Fachbereich 06
Rechtswissenschaft

Vielen Dank für die Aufmerksamkeit

Prof. Dr. Dennis-Kenji Kipker
Professor für IT-Sicherheitsrecht
Universität Bremen
kipker@uni-bremen.de
0421 5905 5465