Sachstand

Das chinesische Internetsicherheitsgesetz

Das chinesische Internetsicherheitsgesetz

Aktenzeichen:	WD 10 - 3000 - 077/19
Abschluss der Arbeit:	27. Januar 2020
Fachbereich:	WD 10: Kultur, Medien und Sport

Inhaltsverzeichnis

1. Vorbemerkung

Dieser Sachstand enthält eine Überblicksdarstellung über das 2017 in Kraft getretene Internetsicherheitsgesetz der Volksrepublik China (CSL)[1].

2. Inhalt und Geltungsbereich des CSL

Das chinesische Internetsicherheitsgesetz, das seit dem 1. Juni 2017 in Kraft ist,[2] trifft Regelungen zu Datenschutz, IT-Sicherheit und Verhalten im Internet.[3] Es gliedert sich in sieben Kapitel:

- Kapitel 1: Allgemeine und bereichsübergreifende Vorschriften
- Kapitel 2: Regellungen zur Unterstützung und Förderung der Netzwerksicherheit
- Kapitel 3: Vorschriften zur Netzwerk-Betriebssicherheit (enthält weitere allgemeine Vorgaben sowie Spezialregelungen für die Betreiber von kritischen Infrastrukturen)
- Kapitel 4: Netzwerk-Informationssicherheit
- Kapitel 5: Monitoring, Frühwarnungen und Notfall-Reaktionsmaßnahmen
- Kapitel 6: Rechtliche Verantwortlichkeit in Cyber-Sicherheitsfragen
- Kapitel 7: Ergänzende Vorgaben[4]

Im deutschen Recht finden sich vergleichbare Inhalte in der Datenschutzgrundverordnung[5] (DSGVO), dem IT-Sicherheitsgesetz[6], den Regelungen zum Äußerungsrecht oder dem Netzwerkdurchsetzungsgesetz[7]. Die chinesische Variante unterscheide sich nach Kessler/Blöchl jedoch in der Anwendung in etlichen Punkten. Grund hierfür sei eine grundsätzlich andere Ausrichtung.

---

1 Auch „Cybersecurity Law“ (CSL) oder „Cybersecurity-Gesetz“ (CSG), seltener „Chinese Cybersecurity Law“ (CCSL).

2 Englische Fassung abrufbar unter URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (Zugriff: 16.01.2020).

3 Kessler, Florian/Blöchl, Jost: So wirkt Chinas Gesetz für Cybersecurity; 22.10.2018; URL: https://www.divsi.de/so-wirkt-chinas-gesetz-fuer-cybersecurity/# (Zugriff: 15.01.2020).

4 Kipker, Dennis-Kenji: Chinese Cybersecurity Law: Neue rechtliche Wege und Umwege nach China, in: Taeger, Jürgen (Hrsg.): Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI; Oldenburg 2019; S. 880 f.

5 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR) (ABl. L 119 vom 4.5.2016, S. 1).

6 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015 (BGBl. I S. S. 1324).

7 Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352).

Argumentierten europäische Gesetzgeber primär mit dem Schutz von Persönlichkeitsrechten ihrer Bürger, stünden in China die Erhaltung der ‚Souveränität über den Cyberspace' und der nationalen Sicherheit im Vordergrund.[8]

Der Anwendungsbereich des CSL erstreckt sich dabei auf natürliche und juristische Personen, die im Gebiet Chinas Informationen erheben, verarbeiten oder verbreiten. Betroffen sind somit auch ausländische Unternehmen mit Niederlassungen in China und ausländische Unternehmen, „die sich zum Beispiel mit ihrer Webseite an chinesische Kunden wenden. Diesen droht bei Verstößen die Blockierung ihrer Angebote in China."[9]

Oberlin beschreibt den Anwendungsbereich ausführlicher wie folgt:

> „Der territoriale Anwendungsbereich gem. Art. 2 CCSL bezieht sich auf das geographische Territorium der Volksrepublik China und ist anwendbar für Unternehmen, die auf dem chinesischen Festland eine geschäftliche Tätigkeit ausführen und somit dort als Niederlassung, Hauptsitz oder unternehmerisch tätige Unternehmung agieren. Der sachliche Anwendungsbereich umfasst den Aufbau eines Netzwerkes, dies bedeutet der Aufbau computerbasierter Kommunikationssysteme. Zudem umfasst Art. 2 CCSL den Betrieb i. S. v. Installation, Verwendung, Überwachung, das zur Verfügung stellen der Infrastruktur, die Instandhaltung i. S. e. Netzwerkwartung, Problem und Störungsbehebung, der Verwendung eines Netzwerkes i. S. d. Benutzung durch die User als Endverbraucher, die Überwachung der Netzwerksicherheit i. S. v. organisatorischen oder technischen Maßnahmen, sowie das Netzwerkmanagement i. S. d. Verwaltung u. a. der Betriebstechnik."[10]

Abbildung 1 stellt den Adressatenbereich des Gesetzes grafisch dar.[11]

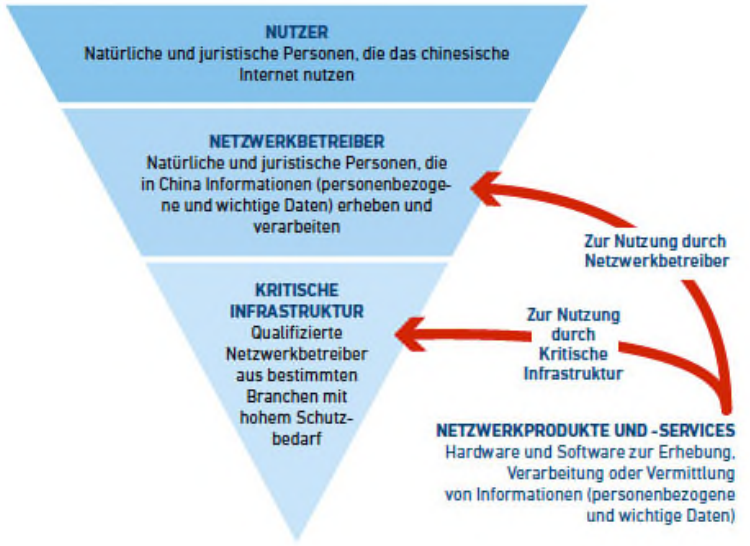
8 Kessler, Florian/Blöchl, Jost: So wirkt Chinas Gesetz…, a.a.O.

9 Ebenda.

10 Oberlin, Jutta Sonja: Neues chinesisches Cyber-Security-Law: Staatliches Kontrollinstrument statt Schutz des Datensubjektes; 10.05.2018; URL: https://www.linkedin.com/pulse/neues-chinesisches-cyber-security-law-staatliches-des-jutta-sonja Zugriff: 16.01.2020). Zitat in Satz 1 korrigiert.

11 Kessler, Florian/Blöchl, Jost: So wirkt Chinas Gesetz…, a.a.O.

Abbildung 1



3. Sonderprobleme und Kooperationspflichten

Nach Kipker bestehen drei zentrale Sonderprobleme im Zusammenhang mit dem CSL:

- Nutzung von VPN[12]-Verbindungen von und nach China:
  „Artikel 5 und 58 CSL eröffnen dem Staat grundsätzliche Befugnisse, Maßnahmen zum Umgang mit Netzsicherheitsrisiken im In- und Ausland zu ergreifen und die Netzwerkkommunikation aus wichtigen öffentlichen Interessen heraus zu beschränken. Hieraus lässt sich die theoretische Möglichkeit ableiten, auch VPN-Verbindungen zu unterbrechen.“[13] Dennoch seien nach Aussage von Kipker auf Grundlage der Vorgaben des CSL bisher keine „flächendeckend und dauerhaft sowie kausal“ signifikanten Einschränkungen von VPN-Verbindungen erfolgt.[14]

- Behördliche Produktüberprüfungen und Zertifizierungen:
  „Gemäß Artikel 23 CSL sind die Anbieter von ‚kritischer Netzwerkausrüstung‘ und ‚spezifischen Cyber-Sicherheitsprodukten‘ verpflichtet, eine behördliche Überprüfung und Zertifizierung ihrer Produkte im Sinne einer Produktzulassung durchzuführen, bevor diese auf dem chinesischen Markt vertrieben werden können. […] Erfasst sind unter anderem

12 Abkürzung für „Virtual Private Network“, deutsch: „virtuelles privates (in sich geschlossenes) Kommunikationsnetz“.

13 Kipker, Dennis-Kenji: Chinese Cybersecurity Law…, a.a.O., S. 883 f.

14 Ebenda, S. 884.

Router, Switches, Server, Firewalls und Anti-Spam-Produkte ab einer katalogmäßig festgelegten Leistungsgrenze. […] Auch im Hinblick auf die Produktzertifizierung existieren zurzeit noch verschiedene offene Fragen […]. Darüber hinaus wird in der Umsetzung der Produktzertifizierung von chinesischer Seite zu klären sein, welche technische Norm für die Zertifizierung welches Produktes einschlägig ist und somit den gültigen Prüfmaßstab bildet."[15]
Artikel 35 CSL regelt den „national security review" für Netzwerkprodukte und -dienste, die im KRITIS[16]-Sektor eingesetzt werden. „Der Cybersecurity Review stellt sich […] als eine Zusammenarbeit zwischen Unternehmen und Behörden dar, wozu Labortests, Betriebsbegehungen, Online-Überwachung und Hintergrundkontrollen gehören. […] Koordiniert wird der Review vom ‚Cybersecurity Review Office', das zugleich auch die Ergebnisse veröffentlichen kann (Artt. 8 und 14). Für den KRITIS-Sektor wird zusätzlich die Zuständigkeit einzelner Fachbehörden bestimmt, Art. 9."[17] Da im Falle des Nicht-Bestehens des Reviews entsprechende Produkte für den chinesischen Markt nicht zugelassen werden sollen, besitzt der Cybersecurity Review eine erhebliche Relevanz für den Marktzutritt.

– Datenlokalisierung:
„Ausgehend vom CSL unterfallen solche Daten, die im Rahmen des Betriebs von kritischen (Informations) Infrastrukturen anfallen, einer Pflicht zur Datenlokalisierung. So wird in Artikel 37 des Gesetzes festgeschrieben, dass derlei Datenbestände grundsätzlich im chinesischen Inland zu speichern sind. Eine Ausnahme wird aber für diejenigen Fälle gemacht, in denen ein Auslandsdatentransfer aus zwingenden Gründen erforderlich ist. Für das Vorliegen dieser Ausnahme übernehmen die betroffenen Unternehmen jedoch selbst die Verantwortung. Unklar ist zurzeit noch, ob sich die Pflicht zur Datenlokalisierung zu Zwecken der Cyber-Sicherheit tatsächlich nur auf die in Artikel 31 CSL definierten kritischen Informationsinfrastrukturen bezieht oder weiter reicht. Eine systematische Auslegung des Gesetzes deutet hier auf ein enges Verständnis hin, wohingegen manche Stimmen behaupten, dass zukünftig sämtliche digitalen und vernetzten Anwendungen, Produkte und Services von der Datenlokalisierung betroffen sind, was erhebliche Auswirkungen vor allem auf für ausländische Unternehmen zur Folge hätte."[18] Unternehmen, die Daten in ein Drittland transferieren wollen, werden „voraussichtlich eine interne Sicherheitsüberprüfung durchführen und bei größeren Datenmengen eine vorherige Genehmigung einholen müssen."[19]
Nach Einschätzung von Pattloch werden die teils sehr weitgehenden Anforderungen an die Beurteilung der Auswirkungen eines Datenexports es im Zweifelsfall Dateninhabern

15 Ebenda, S. 884 f.

16 Abkürzung für „Kritische Infrastrukturen".

17 Kipker, Dennis-Kenji/Müller, Sven: Internationale Cybersecurity-Regulierung, in: InTeR: Zeitschrift zum Innovations- und Technikrecht - 7 (2019); S. 23.

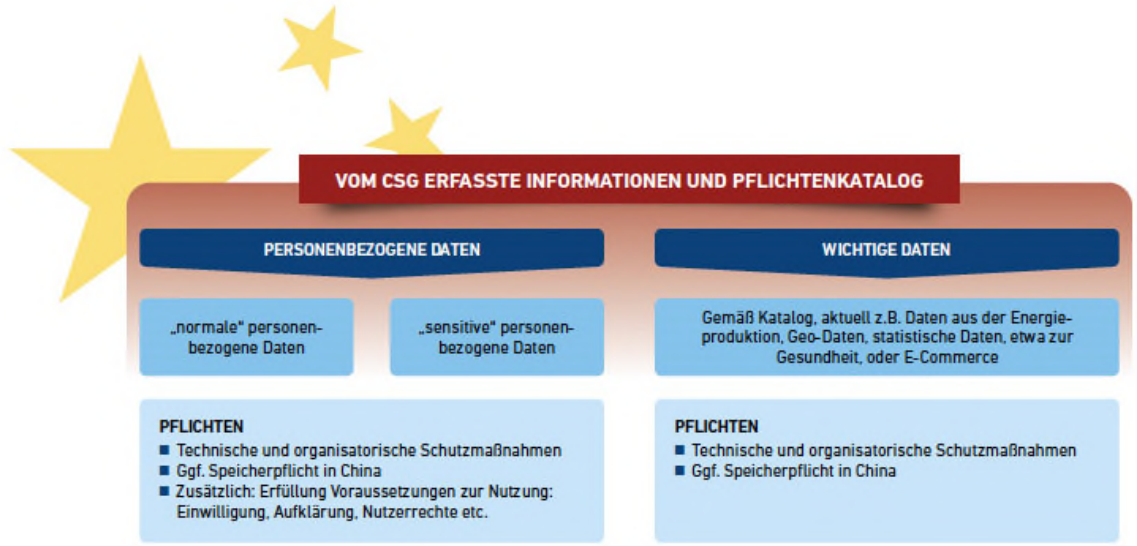
18 Kipker, Dennis-Kenji: Chinese Cybersecurity Law…, a.a.O., S. 885.

19 Kessler, Florian/Blöchl, Jost: So wirkt Chinas Gesetz…, a.a.O.

schwer machen, „ein Netzwerk in China zu betreiben und einen gesetzeskonformen Datenexport ohne behördliche Bestätigung nachzuweisen. Es entsteht ein indirekter Druck, auch als bloßer Netzwerkbetreiber die hohen Anforderungen einer Sicherheitsüberprüfung in möglichst großen Umfang zu erfüllen und sämtliche Anstrengungen zur Selbstprüfung und zum Datenschutz zu dokumentieren.“[20]

Eine Kategorisierung der Datentypen zeigt Abbildung 2.[21]

Abbildung 2



Die Umsetzung des Gesetzes soll für ausländische Unternehmen mit Schwierigkeiten verbunden sein. Gründe hierfür seien die Regelungsflut, fehlendes geschultes Personal oder Abweichungen von geschriebenem Gesetz und Praxis. Chinesische Internet-Unternehmen wie Alibaba oder Jingdong würden in der Praxis (offenbar mit Duldung der Aufsichtsbehörden) einen von den hart formulierten Anforderungen eines empfohlenen Standards abweichenden Weg einschlagen und ließen sich z.B. bei der Registrierung auf ihren Plattformen weitreichende Einwilligungen zusichern.[22]

Für Technologie-Unternehmen könne das CSL somit wie bereits erwähnt zu einer erheblichen Marktzugangseinschränkung führen. Dies betreffe vor allem Anbieter im Bereich Industrie 4.0. Der Begriff der „wichtigen Daten“ würde womöglich viele Informationen aus dem Bereich der

20 Pattloch, Thomas: Update zum Cyber Security Law in China; URL: https://www.plattform-innovation.de/files/Update%20zum%20CSL%20in%20China%20Layout-Pattloch.pdf (Zugriff: 16.01.2020); S. 3.

21 Kessler, Florian/Blöchl, Jost: So wirkt Chinas Gesetz…, a.a.O.

22 Ebenda.

industriellen Fertigung erfassen. Diese potenzielle Marktzugangsbeschränkung habe laut Kessler/Blöchl vor allem mit einer Besonderheit nationaler Standards zu tun. Standards würden in der Regel zur Einhaltung empfohlen und nicht als verpflichtend erlassen. Das CSL fordere aber, dass „zwingende Anforderungen relevanter nationaler Standards“ einzuhalten seien. Häufig würden empfohlene Standards faktisch verpflichtend, weil die Einhaltung von Aufsichtsbehörden, Prüfstellen oder Vertragspartnern gefordert werde. Betreiber Kritischer Infrastrukturen seien so nach dem CSL gezwungen, nur Netzwerkprodukte und -services einzukaufen, für die die Einhaltung relevanter Standards in Sicherheitsüberprüfungen nachgewiesen sei.[23]

Die Sanktionen für Unternehmen und Netzwerkbetreiber sind ebenfalls durch das CSL geregelt. Hierbei können sowohl Netzwerkbetreiber und Unternehmen, als auch die für sie handelnden Personen zur Rechenschaft gezogen werden. „Für Gesetzesverstöße sind sowohl Geldbußen bis ca. 130.000 EUR, als auch weitere Strafen, wie der Entzug bestimmter Lizenzen, die Suspendierung der Geschäftsaktivitäten, sowie die vollständige Einstellung der Geschäftstätigkeit der Netzwerkbetreiber vorgesehen.“[24]

****

23 Ebenda.

24 Oberlin, Jutta Sonja: Neues chinesisches Cyber-Security-Law…, a.a.O.