Cybersicherheit: Wie geht es weiter?

Bereits im Herbst 2017 war das Cybersicherheitsgesetz Thema eines „APA aktuell“-Beitrags in ChinaContact. Nachfolgend ein Update zu diesem Thema, das den derzeitigen Stand beschreibt sowie alte und neue Hindernisse aufzeigt.

Das Cybersicherheitsgesetz in China ist zum 1. Juni 2017 in Kraft getreten. Die Einführung eines solchen Gesetzes, wenn auch aus teilweise nachzuvollziehender Motivation und einem anzuerkennenden Regulierungsbedarf heraus entstanden, hat dennoch von Anfang an bei ausländischen Unternehmen in China für Unruhe gesorgt. Zu Beginn mag das Bewusstsein für die eigene Betroffenheit noch nicht bei allen Unternehmen ausgeprägt gewesen sein. Es herrschte die Vorstellung vor, dass in erster Linie Unternehmen aus dem IT- und Software-Bereich von einem solchen Gesetz betroffen sind. Im Laufe der letzten 18 Monate hat sich jedoch die Erkenntnis durchgesetzt, dass die allermeisten in China tätigen Unternehmen in der einen oder anderen Form von den Regelungen des Cybersicherheitsgesetzes betroffen sind. Offen bleibt in vielen Fällen die Frage, wie stark einzelne Unternehmen in ihrer Geschäftstätigkeit durch das Gesetz beeinflusst werden. Laut der aktuellen Geschäftsklima-Umfrage der Deutschen Handelskammer in China bewerten immerhin 44 Prozent der befragten Unternehmen das Cybersicherheitsgesetz im Bereich „Schutz kritischer Informationen“ als negativ für ihre Wettbewerbsfähigkeit in China, 48 Prozent sind sich unsicher.

Was genau hat sich seit dem letzten „APA aktuell“-Bericht zu diesem Thema (ChinaContact 10/2017) getan? Welche alten und neuen Hindernisse bestehen? Wie reiht sich der Prozess um die Ausgestaltung des Gesetzes in die über allem liegende ideologische Festlegung der Partei und Xi Jinpings bei den Themen Nationale Sicherheit und Cybersicherheit ein,

Sicherheit oder Mittel um zur „Cyber-Supermacht“ aufzusteigen? Ein Problem des Gesetzes sind die oftmals unspezifischen Termini.

Foto: iStock © loveguli

vor allem vor dem Hintergrund, dass China den Status einer „Cyber-Supermacht“ anstrebt? Und wie stark kann der Fokus auf dem Aufbau einer nationalen Gesetzgebung liegen, wenn eigentlich immer klarer wird, dass Sicherheitsfragen und Datenflüsse im Zeitalter von Digitalisierung und Industrie 4.0 nicht an Grenzen haltmachen? Eine Vielzahl von Fragen, die sich nicht abschließend beantworten lassen, die an dieser Stelle aber immer wieder aufgegriffen und einem kritischen Blick unterworfen werden sollen.

Was ist seit Juni 2017 passiert?

Seit Inkrafttreten des Gesetzes zählt die Europäische Handelskammer in China (EUCCC) an die 50 Ausführungsbestimmungen, Regulierungen und Standards mit direktem Bezug zum Cybersicherheitsgesetz, die auf den Weg gebracht wurden und größtenteils bereits in Kraft sind. Dennoch fehlt in wichtigen Fragen weiterhin Klarheit und es ist nicht abzusehen, ob wirklich bis Ende 2018 alle Ausführungsbestimmungen formuliert sind. Ebenfalls offen bleibt, wie viel Zeit den Unternehmen dann noch bleibt, um die Regelungen umzusetzen. Ein bekanntes und viel diskutiertes Problem des Gesetzestextes sind die oftmals unspezifischen Termini, beispielsweise „wichtige Daten“, „kritische Informationsinfrastruktur“ oder „nationale Sicherheit“. Diese Unschärfen sowie die weitere Ausgestaltung des Gesetzes sollten – laut Ankündigung der chinesischen Regulierer – durch konkrete Ausführungsbestimmungen bis spätestens Ende 2018 festgelegt, definiert und geklärt werden. Diese Klarheit ist für Unternehmen von immenser Bedeutung, hängen damit doch direkte Investitionskosten zusammen. Hinzu kommt zum Beispiel für deutsche Unternehmen, die in China Forschung und Entwicklung betreiben, dass sich durch Anforderungen wie lokale Datenspeicherung und einen stark regulierten grenzüberschreitenden Datenverkehr umfassende Herausforderungen ergeben, die unter Umständen den Standort China für F&E-Projekte unattraktiver machen. Leider fehlen auch in diesem Bereich immer noch zahlreiche Details.

Cybersicherheit und das Cybersicherheitsgesetz ziehen sich seit 2017 als Thema durch zahlreiche deutsch-chinesische Foren und Gesprächsrunden, angesprochen meist von deutscher Seite. Stellvertretend genannt seien hier der deutsch-chinesische Cyberkonsultationsmechanismus und die Deutsch-Chinesische Kommission Normung sowie politische Termine wie die Deutsch-Chinesischen Regierungskonsultationen und bilaterale Besuche in China und Deutschland. Die EUCCC begleitet über eine eigene Arbeitsgruppe den Prozess in China über Kommentierungen neuer Regelungen und einen engen Austausch mit den chinesischen Behörden. Auch auf politischer EU-Ebene gibt es eine Reihe von etablierten Formaten, unter anderem den „ICT Dialogue with China“ und eine Cyber Task Force. Darüber hinaus ist eine Vielzahl an Analysen unterschiedlichster internationaler Institutionen zur Frage der Auswirkungen des Gesetzes auf Unternehmenstätigkeiten erschienen, als Beispiel sei hier das Center for Strategic and International Studies (CSIS) genannt.

Großer Spielraum für Behörden

Erst kürzlich hat in Peking das zweite Industrie-4.0-Symposium stattgefunden. Bei dem Anlass haben die anwesenden politischen Vertreter des Bundesministeriums für Bildung und Forschung (BMBF) und des Bundeswirtschaftsministeriums (BMWi) noch einmal ausdrücklich die Probleme mit Datenlokalisierungsauflagen und grenzüberschreitendem Datenverkehr vor allem im Zusammenhang mit Industrie 4.0 angesprochen. Der chinesischen Regierung dürfte das Interesse der Wirtschaft an den Details des Cybersicherheitsgesetzes also inzwischen sehr deutlich vor Augen geführt worden sein. Aber erst im Verlauf des Jahres 2019 und danach wird sich zeigen, wie genau eine Umsetzung der einzelnen Bestimmungen erfolgen kann und inwieweit Unternehmen in ihrer Tätigkeit beeinflusst werden. Es wird, nach Einschätzungen vieler westlicher Experten, ein großer Ermessens- und Handlungsspielraum bei den einzelnen Behörden verbleiben, was weiterhin für Unsicherheit sorgen wird. Eventuell wird ja auch noch ein weiterer zeitlicher Puffer geschaffen und die Umsetzung verschoben, ähnlich der Verschiebung des Verbots von nicht-chinesisch zertifizierten VPN-Tunneln auf März 2019. In der Begründung dafür wurde damals auf die Komplexität der Aufgabe verwiesen. Ein Hinweis, der auch für das Cybersicherheitsgesetz gelten kann.

Es ist in letzter Zeit immer deutlicher geworden, dass der Umgang mit Daten, dem Kern aller Debatten um Cybersicherheit, nicht allein auf nationaler Ebene im „luftleeren Raum“ geregelt werden kann. Die Entwicklungen der Digitalisierung passieren schnell und zeitgleich weltweit, und das schneller, als Regierungen und Unternehmen sich zu Themen wie zum Beispiel dem grenzüberschreitenden Datenverkehr positionieren können. Von Seiten der Politik besteht weiterhin dringender Handlungsbedarf, mit der chinesischen Regierung auf einen Nenner zu kommen. In erster Linie, damit sich regulatorische Asymmetrien zwischen den unterschiedlichen Cyber-Regimen nicht zum Nachteil für die deutschen Unternehmen entwickeln und Geschäftspotenzial unnötig eingeschränkt wird.

APA-Geschäftsführung China:
Ferdinand Schaff
f.schaff@apa.bdi.eu / Telefon +49 30 2028 1409
Patricia Schetelig
P.Schetelig@bdi.eu / Telefon +49 30 2028 1532
www.asien-pazifik-ausschuss.de

Asien-Pazifik-Ausschuss
der Deutschen Wirtschaft