

Chinas Data Security Law – Basis für moderne Datenökonomie?

Am 3. Juli 2020 veröffentlichte der NVK den Entwurf eines Datensicherheitsgesetzes (Data Security Law, DSL). Zum ersten Mal formuliert China damit ein Gesetz, das verschiedene Aspekte von Datenschutz und -sicherheit sowie Datennutzung zusammenführt. Der Entwurf markiert einen Kurswechsel, weg von einem engen Fokus auf nationale Sicherheit und hin zu einem mehrgleisigen Ansatz, bei dem Sicherheitsbedenken und wirtschaftliche Vorteile gegeneinander abgewogen werden.

Technologieunternehmen gedeihen durch die Sammlung und Auswertung von Daten. Große Datensätze können verwendet werden, um Herstellungsprozesse zu verbessern, bessere Medikamente zu entwickeln oder Algorithmen zu trainieren, um nur einige Beispiele zu nennen. Die Nachfrage nach Daten ist enorm und China ein besonders großer Markt dafür. Schätzungen der International Data Corporation zufolge wird die Menge der in China erstellten, gesammelten oder kopierten Daten bis 2025 von 7,5 Zettabytes im Jahr 2018 auf 48,6 Zettabytes ansteigen. Das entspricht 27,8 Prozent der weltweiten Datenmenge. Zum Vergleich: Die USA werden im gleichen Zeitraum 17,5 Prozent der weltweit generierten Gesamtdaten ausmachen.

In den vergangenen Jahren haben die Geschäfte mit Daten in China rasant zugenommen. Dabei spielte sich ein Großteil des chinesischen Datenmarktes in wenig regulierten Grauzonen ab. Bislang konzentrierten sich die Behörden vor allem darauf, illegalen Handel zu unterbinden sowie zu regeln, welche Daten wie ins Ausland übertragen werden dürfen. Auch der Schutz persönlicher Daten von Einzelpersonen wurde durch Regulierungen und nationale Standards weiterentwickelt. Das sich in Arbeit befindende Personal Information Protection Law soll in diesem Bereich eine neue Grundlage schaffen.

Die großen, anonymisierten Datensätze, die als Treibstoff für Algorithmen und Big-Data-Anwendungen gehandelt werden, sind aber nach wie vor unzureichend verwaltet. Das DSL ist ein großer Schritt in Pekings Bemühen, einen gesetzlichen Rahmen für eine moderne Datenökonomie in China zu schaffen.

Chinas Legislative will mit dem DSL Ordnung in bisherige Patchwork-Regulierungen des chinesischen Datensektors bringen.



Foto: imago images / VCG

fen. Der Gesetzentwurf für das DSL zielt auf alle innerhalb der Volksrepublik durchgeführten Datenaktivitäten. Der Schwerpunkt des DSL liegt dabei auf nicht personenbezogenen Daten. Auf internationaler Ebene bringt das DSL Daten in eine koordinierte Handelsstrategie ein, die durch selektive Reziprozität und Protektionismus gekennzeichnet ist.

Chinas Legislative zielt mit dem DSL darauf ab, Ordnung in die bisherigen Patchwork-Regulierungen des chinesischen Datensektors zu bringen. Allerdings bleibt der Entwurf an vielen Stellen noch zu unspezifisch. Generell bedeutet der Gesetzentwurf für Akteure im Datenraum zusätzliche Regeln und die Abschaffung eines Teils des bisher unregulierten Handels.

Offene Fragen für ausländische Unternehmen

- Nationale Sicherheit und extraterritoriale Reichweite**
 Insbesondere der breite Geltungsbereich und die extraterritoriale Reichweite des DSL bergen besondere Risiken für ausländische Unternehmen. Der Gesetzentwurf räumt den zuständigen chinesischen Behörden im Namen der nationalen Sicherheit weitreichende Befugnisse ein, auf Daten zuzugreifen und die für die Datenverarbeitung Verantwortlichen zu regulieren. Rechtliche Haftungsansprüche können auch gegen Organisationen oder Einzelpersonen außerhalb der Volksrepublik geltend gemacht werden, die Datenaktivitäten durchführen, welche „die nationale Sicherheit, das öffentliche Interesse oder die legitimen Interessen von Bürgerinnen, Bürgern und Organisationen Chinas gefährden“. Eine so breite Bestimmung könnte internationale Unternehmen beträchtlichen Rechtsunsicherheiten aussetzen.
- Datendefinition**
 Nach Artikel 3 des Gesetzentwurfs werden „Daten“ allgemein definiert als „alle elektronischen oder nichtelektronischen Aufzeichnungen von Informationen“. Problematisch ist in diesem Zusammenhang zum einen die Verschmelzung der Begriffe „Daten“ und „Informationen“, welche die Auslegung des Gesetzes in Rechtsstreitigkeiten erschweren dürfte. Außerdem nimmt der Entwurf keine ausreichende Trennung zwischen personenbezogenen und nicht personenbezogenen Daten vor. Statt erstere dem eigens hierzu in Arbeit befindlichen Personal Information Protection Law zu überlassen, besteht die Gefahr weiterer Unklarheiten und fehlender Rechtssicherheit.
- Fehlende Präzisierung**
 Viele Begriffe und Vorgaben sind zudem wenig spezifisch beziehungsweise vage formuliert. So sind beispielsweise Schulungen „regelmäßig“ durchzuführen (Artikel 28), aber ob dies wöchentlich oder jährlich bedeutet, ist aktuell nicht geklärt. Gleiches gilt für die Frage, welche Unternehmen als „Operator“ zählen (Artikel 31).

Geopolitik – Datenhandel als Druckmittel

Auf geopolitisch-strategischer Ebene dürfte das Data Security Law zu größeren Umwälzungen führen. So ermöglicht der Entwurf, den Datenzugang als Druckmittel bei Handelsstreitigkeiten einzusetzen und führt an, dass China beim Handel mit Datenbeständen entsprechende Maßnahmen ergreifen wird. Jedes Land, das wegen der chinesischen Datenpraktiken

Verbote oder Beschränkungen für chinesische Investitionen oder den Handel erlässt, könnte dieser „Tit-for-Tat“-Datendiplomatie unterliegen. In der Praxis könnte China unter dieser Klausel den Datenexport in viele westliche Länder einschränken. Die EU hat zum Beispiel mit „gleichgesinnten“ Ländern wie Japan, Kanada und Israel Abkommen geschlossen, die einen freien Datenfluss vorsehen. Zwischen der EU und ihrem „systemischen Rivalen“ China wurde ein solches Abkommen bisher nicht unterzeichnet, sodass die Übertragung europäischer Daten in die Volksrepublik beschränkt ist. Auf Grundlage des DSL könnte der Fluss chinesischer Daten nach Europa in gleichem Maße beschränkt werden.

Mit Blick auf Hongkong ist das DSL kritisch zu betrachten. Da das DSL auf Daten innerhalb des Hoheitsgebiets der Volksrepublik China Anwendung findet, ohne Einschränkung für die beiden Sonderverwaltungsregionen, würde es sowohl für Daten auf dem chinesischen Festland als auch in Hongkong und Macao gelten. In dieser Hinsicht würde der Gesetzentwurf den Autonomiestatus Hongkongs, der bereits durch das „Gesetz zum Schutz der nationalen Sicherheit in der Sonderverwaltungsregion Hongkong“ vom 30. Juni 2020 abgeschwächt wurde, weiter verringern.

Zukunft der Datenwirtschaft in und mit China

Letztlich bleibt abzuwarten, ob der Gesetzentwurf zu einem mehr oder weniger restriktiven Umfeld für den Datenhandel in und mit China führen wird. Das DSL eröffnet nach aktuellem Stand Raum für Flexibilität, indem es den Regionalregierungen und sektoralen Regierungsabteilungen die Entscheidung darüber überträgt, welche Daten als „wichtige Daten“ eingestuft werden sollen. Vieles hängt daher von der Umsetzung durch die Zentral- und Lokalregierungen ab. Möglich wäre, dass Provinzen um die Ansiedlung von Unternehmen konkurrieren werden, indem sie die Beschränkungen für den digitalen Handel senken. Die Provinz Hainan hat ein solches Programm bereits angekündigt. Allerdings dürfte eine geografisch und sektoral uneinheitliche Regulierung von „wichtigen Daten“ für ausländische Unternehmen auch erhebliche Unsicherheiten und beträchtlichen Mehraufwand bedeuten.

Gegenwärtig liegt die Volksrepublik am unteren Ende des Digital Services Trade Restrictiveness Index der OECD. Es ist unwahrscheinlich, dass der neue Gesetzentwurf dieses Ranking in größerem Umfang verbessern 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

