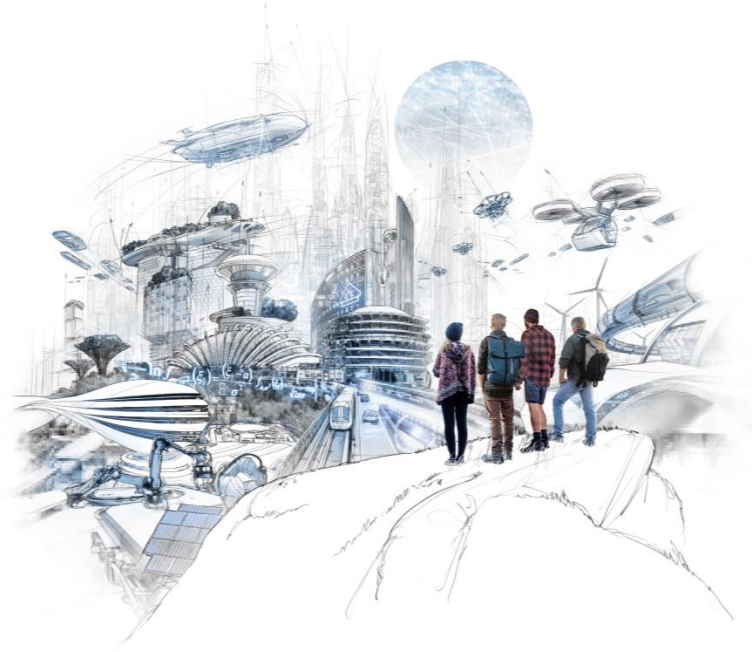
Zusammenfassung Chinese Cryptography Law



China: Neue Vorgaben zur Cybersicherheit – Entwurf des Kryptografiegesetzes veröffentlicht

Seit der Vorstellung der letzten, weit gefassten Entwurfsfassung des chinesischen Kryptografiegesetzes aus April 2017 gab es vermehrt Spekulationen über Inhalte und Relevanz des Chinese Cryptography Law, das sich als Begleitregelung zum chinesischen Cyber-Sicherheitsgesetz (CSL) aus 2016 versteht. Jüngst wurde am 5. Juli 2019 der überarbeitete Entwurf veröffentlicht, der noch bis zum 2. September 2019 zur Kommentierung offensteht. Zentrale Zielsetzung des Gesetzes ist nach wie vor die Entwicklung neuer kryptografischer Verfahren, Dienste und Produkte in China und die damit verbundene Stärkung der IT- und Datensicherheit, daneben steht wie für das CSL auch der Schutz von öffentlichen und nationalen Sicherheitsinteressen im Vordergrund.
Systematisch ist der aktuelle Entwurf mit 44 Artikeln in fünf Abschnitte untergliedert: General Provisions (Kapitel 1), Core Cryptography and Ordinary Cryptography (Kapitel 2), Commercial Cryptography (Kapitel 3), Legal Liability mit umfassenden Sanktionsregelungen sowohl für öffentliche wie auch für private Stellen (Kapitel 4) und Supplemental Provisions (Kapitel 5).

Unterscheidung zwischen verschiedenen kryptografischen Verfahren

Art. 2 des Entwurfs definiert „Kryptografie" vornehmlich als Produkt, Technologie oder Dienst, der effektiven Schutz von Informationen durch Verschlüsselung gewährleistet. Politisch wird ein einheitlicher, staatsweiter Ansatz verfolgt, um zentrale Prinzipien und Leitlinien zu bestimmen. Zuständig ist dabei laut dem Vorschlag landesweit eine zentrale Behörde, die auf Bezirksebene durch weitere Verwaltungsbehörden unterstützt wird. Als Staatsaufgabe verstanden, bedeutet Förderung von Kryptografie auch, dass herausragende Forscher auf diesem Gebiet eine staatliche Auszeichnung erhalten, und die Weiterentwicklung der Technologie sowohl im Bildungssektor als auch in den staatlichen Wirtschafts- und Sozialplänen angemessene Berücksichtigung findet.
Nach Art. 6 wird zwischen unterschiedlichen kryptografischen Verfahren unterschieden, der „Core Cryptography", „Ordinary Cryptography" sowie der „Commercial Cryptography". Erstgenannte Verfahren sollen in erster Linie zum Schutz von Staatsgeheimnissen der Klassen „top secret" und „secret" eingesetzt werden. Dementsprechend sind die beiden vorgenannten Verfahren auch selbst als Staatsgeheimnisse einzustufen. „Commercial Cryptography" hingegen dürfte im Einsatz deutlich breitere Anwendungsfelder haben, da hiermit per Definition alle sonstigen Informationen geschützt werden sollen, die keine Staatsgeheimnisse sind. Aufgrund dieses breiten Anwendungsbereichs richten sich entsprechende Produkte, Dienste und Vorgaben an natürliche und juristische Personen oder andere Einrichtungen, die zu Zwecken der Informationssicherheit kryptografische Verfahren einsetzen. Gesetzlich wird gem. Art. 12 der Diebstahl verschlüsselter Daten, der Einbruch in kryptografische Systeme und der Einsatz von Kryptografie zu illegalen Zwecken sanktioniert.

„Core Cryptography“ und „Ordinary Cryptography“ als Staatsaufgabe

Die Entwicklung und der Einsatz von Verfahren der „Core Cryptography“ und „Ordinary Cryptography“ sind vorrangig Staatsaufgabe. Staatsgeheimnisse sind, unabhängig von der technischen Art der Datenübermittlung, stets mit vorgenannten Verfahren zu verschlüsseln. Jede Einrichtung, die Zugang zur Core und Ordinary Cryptography hat und hiermit arbeitet, unterliegt der Geheimhaltung und wird durch zuständige Verwaltungsbehörden überwacht, unangekündigte Sicherheitsüberprüfungen sind für letztgenannten Fall möglich. Sicherheitslücken sind unverzüglich zu melden und Gegenmaßnahmen zu ergreifen, entsprechende Vorkehrungen werden auch hier wieder staatlich gefördert.

Offener Wettbewerb für kommerzielle kryptografische Produkte, Einbindung der Standardisierung

Für kommerziell nutzbare kryptografische Produkte bestimmt Art. 21 des Gesetzentwurfs sogleich, dass der Staat einen offenen und wettbewerbsorientierten Markt fördern soll, um entsprechende Industriezweige zu unterstützen. Wo einerseits marktwirtschaftliche Offenheit proklamiert wird – in Art. 30 beispielsweise ist gar von „Selbstregulierung“ die Rede –, wird andererseits weitergehend die Aussage getroffen, dass die Entwicklung, Herstellung oder der Import und Export kryptografischer Produkte unter anderem nicht die Interessen nationaler Sicherheit oder der Öffentlichkeit beeinträchtigen darf – wo hier die genaue Grenze zu ziehen ist, wird jedoch offengelassen: Hier würde es wohl wie für das CSL auch vorwiegend auf untergesetzliche konkretisierende Regelungen ankommen. Das nicht fehlen dürfende Thema Standardisierung wird ab Artikel 22 aufgegriffen. So ist es staatliche Aufgabe, ein System zur Entwicklung von kommerziellen kryptografischen Standards zu begründen und zu verbessern, damit entsprechende nationale Standards und Industriestandards entwickelt werden können. Darüber hinaus fördert der Staat soziale Netzwerke und Unternehmen, die über dem herkömmlichen Niveau liegende Standards entwickeln. Art. 23 des Gesetzentwurfs bestimmt, dass sich China ebenso an Aktivitäten internationaler Standardisierung im Bereich von kommerzieller Kryptografie beteiligt, hierzu gehört auch die Konvertierung chinesischer Standards in ausländische Standards, und umgekehrt. Im Rahmen der Standardisierungsaktivitäten sollen unter anderem Firmen, die bereits genannten sozialen Netzwerke und Bildungs- sowie Forschungseinrichtungen einbezogen werden. Gem. Art. 25 fördert der Staat außerdem die Anwendung von freiwilligen Standards zur kommerziellen Kryptografie. Das Gesetz greift ebenfalls die Überprüfung und Zertifizierung kommerzieller kryptografischer Produkte auf. Hierzu soll ein wohl zunächst freiwilliges System einschließlich der erforderlichen technischen Spezifikationen entwickelt werden. Bezug nimmt der Gesetzentwurf außerdem auf Zufallskontrollen, eine „vereinheitlichte Informationsplattform“ zur Verwaltung von kommerziellen kryptografischen Produkten und das Social Credit-System der Volksrepublik China.

Kryptografie mit Bezügen zur nationalen Sicherheit, „Critical Network Equipment“

Der Begriff „Critical Network Equipment“ ist bereits aus dem CSL bekannt und wird aufgrund der engen inhaltlichen Bezüge des Gesetzes zur Cybersicherheit auch im Entwurf des Chinese Cryptography Law verwendet. So soll gelten, dass jedes kommerzielle kryptografische Produkt, das einen Bezug zur nationalen Sicherheit oder Wirtschaft oder zu einem sonstigen öffentlichen Interesse aufweist, in die Liste für „Critical Network Equipment“ aufgenommen wird, und nur nach Durchführung einer Sicherheitsüberprüfung auf dem Markt zur Verfügung gestellt werden kann. Vergleichbare Regelungen gelten für kryptografische Dienste. Ebenso aus dem CSL bekannt ist die „Critical Information Infrastructure“ (CII). Betreiber von CII sollen Kryptografie zum Schutz der Aufrechterhaltung ihrer Funktionsfähigkeit einsetzen, und im Zuge des Einsatzes Sicherheitsbewertungen durchführen. In diesem Zusammenhang wird der auch aus dem CSL bekannte „National Security Review“ angeführt, der nicht nur für CII, sondern auch für solche Produkte und Dienste relevant ist, die einen Bezug zur kommerziellen Kryptografie aufweisen, und von staatlichen Einrichtungen genutzt werden. Welche Einrichtungen und Produkte im Einzelnen unter diese offen gewählte Formulierung fallen, bleibt zunächst unklar.

Import- und Exportbeschränkungen für kryptografische Produkte

Soweit Fragen der nationalen Sicherheit oder des öffentlichen Interesses betroffen sind, werden wie auch schon für das CSL Kontrollregelungen bestimmt, die die Ein- und Ausfuhr von Produkten regeln. In diesem Sinne schreibt Art. 28 des Entwurfs vor, dass eine Liste kommerzieller Kryptografieprodukte zu erstellen ist, die Importlizensierungen und Ausfuhrbeschränkungen enthält. Die Liste wird in Zusammenarbeit des Commerce Department des State Council, der Cryptographic Administrative Authority und der General Administration of Customs erstellt. Die Regelungen zu Import- und Exportbeschränkungen gelten jedoch nicht für Verbraucherprodukte.

buchachon / Fotolia

Fazit und Ausblick

Die inhaltlichen Vorgaben des neu vorgelegten Entwurfs des chinesischen Kryptografiegesetzes halten sich im Rahmen des zu Erwartenden. Mit der an verschiedenen Punkten stattfindenden Verschränkung zum CSL wird nochmals deutlich, dass sich das Cybersecurity Law stärker als allgemeine Rahmengesetzgebung versteht, die durch bereichsspezifische Vorgaben zunehmend ergänzt, konkretisiert und ausgebaut wird. Gleichwohl ist auch der gegenwärtige Entwurf des Cryptography Law verschiedentlich durch offene Formulierungen gekennzeichnet, die auch für die Anwendung dieses Gesetzes wieder Unsicherheiten schaffen werden – dies betrifft insbesondere auch den Umfang der Einbeziehung von Normen und Standards. Das weite Anwendungsfeld kommerziell genutzter kryptografischer Produkte und die damit verbundene Kategorisierung von Import- und Exportbeschränkungen macht auch dieses Gesetz – wie schon das CSL – für außerhalb von China tätige Unternehmen relevant.

Dr. Dennis-Kenji Kipker
Legal Advisor IT-Sicherheits- und Datenschutzrecht

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Stresemannallee 15
60596 Frankfurt am Main
Tel. +49 151 40223163