Redaktion MMR-Aktuell Kurzbeiträge/Kommentare MMR-Aktuell 2015, 370972

Stellungnahme zum aktuellen Entwurf des Peopleâ€™s Republic of China Cybersecurity Law

Dr. Dennis-Kenji Kipker ist Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen.

Diese Stellungnahme zum aktuellen Entwurf des People's Republic of China Cybersecurity Law untersucht die wesentlichen rechtlichen Besonderheiten, die sich aus den einzelnen Kapiteln des Gesetzgebungsvorhabens ergeben und vergleicht diese mit den Regelungen aus dem IT-SiG und der NIS-RL. Für einzelne Probleme werden entsprechende Lösungsvorschläge bzw. Ergänzungen zum Entwurf skizziert. Die inhaltlichen Ausführungen basieren auf der Übersetzung von Chinalawtranslate i.d.F. v. 9.7.2015.

Zu Chapter 1: General Provisions

Kapitel 1 des Cybersecurity Law (im Folgenden bezeichnet als Gesetzentwurf) bestimmt die generelle Zielrichtung des Gesamtvorhabens. So wird festgelegt, dass der Zweck des Gesetzes vor allem in der Sicherstellung der Netzwerksicherheit, der Wahrung nationaler öffentlicher und Sicherheitsinteressen und im Schutz der Rechte und Interessen von Bürgern, Rechtspersonen und anderen vergleichbaren Organisationen liegt, was auch dem beschlossenen IT-SiG für Deutschland sowie der im Trilog befindlichen NIS-RL der EU nahe kommt. Die ausdrücklichen Anforderungen des chinesischen Gesetzentwurfs gehen jedoch noch weiter, indem festgestellt wird, dass auch sichergestellt werden soll, dass die „Herrschaft über den digitalen Raum" erhalten bleibt. Der Anwendungsbereich des Gesetzes bezieht sich geografisch auf Festlandchina und umfasst vom Sachbereich alle Vorgänge von der Konstruktion eines Netzwerks bis hin zu dessen Kontrolle und Instandhaltung.

Dem chinesischen Staat fällt dabei die Hauptaufgabe zu, geeignete Mechanismen zu entwerfen, um die gesamtheitliche Netzwerksicherheit zu gewährleisten, aber auch das Bewusstsein für IT-Sicherheit in der Öffentlichkeit zu stärken, was wiederum mit den Aufgaben des *BSI* aus dem IT-SiG zu vergleichen ist. Auch nach dem chinesischen Gesetzentwurf soll ein transnationaler Austausch über Netzwerktechnologie und -sicherheit stattfinden mit dem Ziel der Schaffung eines sicheren, offenen und gesamtheitlich verfassten digitalen Raums. Zuständig für die Umsetzung dieser Maßnahmen sind verschiedene Behörden auf unterschiedlichen Ebenen, es soll also keine zentrale Stelle benannt werden, wie es in der deutschen Gesetzgebung der Fall ist: Zwar wird dem „State Information department" eine generelle Zuständigkeit zugeschrieben, diese wird aber ergänzt um Kompetenzen für das „State Council Ministry of Industry and Information Technology", daneben werden auch Behörden im Bereich der darunter liegenden Verwaltungsbezirke über Zuständigkeiten verfügen. Der Gesetzentwurf erlaubt, ausgehend von seiner Zielsetzung und entsprechend dem europäischen Schutzstandard, die Aufnahme von Industriestandards u.a. zur Gewährleistung der Integrität von Online-Daten. Hier dürfte eine Vergleichbarkeit mit der Aufnahme technischer Normen und Standards in unbestimmte Rechtsbegriffe im deutschen Recht bestehen. Zur Regulierung der Netzwerksicherheit werden über den Staat hinaus private Interessenverbände einbezogen.

Auffallend ist, dass der Gesetzentwurf über seine technischen Sicherheitsverpflichtungen hinaus auch

ethische Vorgaben für die Nutzung digitaler Netzwerke enthält. Sowohl für natürliche Personen wie auch für Organisationen wird eine Meldemöglichkeit an nationale Behörden sichergestellt, wenn es um Belange der Netzwerksicherheit geht.

Zu Chapter 2: Network Security Strategy, Planning and Promotion

Das zweite Kapitel bestimmt vornehmlich, wie die in Kapitel 1 definierten Ziele durch eine nationale „Netzwerksicherheitsstrategie" umgesetzt werden sollen. Manche der Vorgaben dieser Netzwerksicherheitsstrategie wirken teils noch etwas abstrakt, was aber auch daran liegen mag, dass der Gesetzentwurf nur den Impuls geben soll, eine solche Strategie zu schaffen, und deshalb nur die grundlegendsten Zielsetzungen festlegen kann. Ähnlich den deutschen und europäischen Bestrebungen soll besonders für KRITIS ein herausgehobenes Schutzniveau geschaffen werden.

Kritische Infrastrukturen werden definiert als Telekommunikation, Radio, Fernsehen, Energie, Verkehrswesen, Wasser und Finanzeinrichtungen, wobei die Definition für weitere Bereiche geöffnet ist, wohingegen auf europäischer Ebene eine geschlossene Definition angestrebt wird, insb. auch, um die Implementierungskosten zu reduzieren und Rechtssicherheit zu schaffen. Die für KRITIS-sensible Bereiche zuständigen „State Council departments" treffen, basierend auf der nationalen Netzwerksicherheitsstrategie, die Aufgabe, eigene Sicherheitspläne zu organisieren und für deren Umsetzung zu sorgen. Einbezogen werden ebenso die in der Verwaltungshierarchie niedriger angesiedelten Provinzen und autonomen Regionen. Nochmals wird an dieser Stelle der zu Deutschland und Europa unterschiedliche Ansatz deutlich, die IT-Sicherheit von KRITIS nicht in die Hände einer zentralen Stelle zu legen. Inwieweit dies der IT-Sicherheit förderlich oder abträglich ist, kann zum jetzigen Zeitpunkt noch nicht konkret beantwortet werden, da auch die nationalen Neuregelungen noch nicht in Kraft getreten und damit ebenso noch nicht etabliert sind. Deutlich ist aber, dass die Verlagerung der Aufgaben auf verschiedene Institutionen zu einer größeren Informationsproliferation führen dürfte, als es in Deutschland der Fall sein wird. In diesem Sinne müssten in jedem Falle geeignete Schutzregelungen vorgesehen werden, damit es zu keiner Zweckentfremdung in der Datenverarbeitung kommt.

Damit die Netzwerksicherheit realisiert werden kann, legt der Staat eine Systematik von Netzwerksicherheitsstandards fest. Damit das IT-Sicherheitsniveau an die technische Entwicklung und damit auch an potenzielle neue Bedrohungslagen angepasst ist, werden diese Standards regelmäßig revidiert. Positiv hervorzuheben ist, dass im Gesetzentwurf auch Ansätze zur endgerätebezogenen IT-Sicherheit vermerkt werden, die in Zukunft eine größere Rolle zur Abwehr von Cybersicherheitsrisiken spielen dürfte. Privatunternehmen sollen ebenfalls in die Festlegung der Sicherheitsstandards einbezogen werden. Auch dies scheint wünschenswert, da durch die Bestimmung branchenüblicher und individueller Standards deutlich mehr Innovationspotenzial in die Abwehr von Cybersicherheitsrisiken eingebracht werden kann. Vorgesehen ist auch, die Rechte des geistigen Eigentums sog. „technology protecting networks" zu schützen. Was genau unter dieser doch recht wichtigen Festlegung zu verstehen sein soll, bleibt aber unklar. Abgerundet wird die nationale Netzwerksicherheitsstrategie Chinas durch staatliche Werbe- und Schulungsmaßnahmen.

Zu Chapter 3: Network Operations Security

Abschnitt 1 des 3. Kapitels sieht konkrete Maßnahmen vor, um die Netzwerksicherheit zu gewährleisten. Insgesamt sind die festgelegten Standards hier recht hoch. Als erste Voraussetzung wird bestimmt, dass der Staat ein vernetztes Schutzsystem bestimmt, um IT-Sicherheit zu gewährleisten. Für Netzwerkdiensteanbieter ergibt sich hieraus eine Reihe umzusetzender Verpflichtungen, deren Verletzung auch bußgeldbewehrt ist (siehe Art. 51 ff.). Für sich genommen sind diese Verpflichtungen allesamt sinnvoll, allerdings fehlt eine Konkretisierung der Vorschriften durch entsprechende technische Vorgaben. Nicht deutlich wird somit, ab wann von der Gesetzeskonformität einer bestimmten technischen Einrichtung gesprochen werden kann. Hier müssen Verweise auf technische Richtwerte festgemacht werden, insb. wenn es um die Implementierung eines ISMS geht. Ebenso betrifft diese Schwäche des Gesetzentwurfs die festgelegte Endgerätesicherheit. Nicht deutlich wird hier, welche die relevanten nationalen und industriellen Standards sein sollen.

Für Produkte, die während ihres Gebrauchs personenbezogene Daten erheben, wird eine Informationsverpflichtung vorgeschrieben. Welche Voraussetzungen an die grds. begrüßenswerte datenschutzrechtliche Einwilligung geknüpft sind, wird aber nicht bestimmt. Hier besteht ebenso Konkretisierungsbedarf bzw. der Verweis auf entsprechende Vorschriften muss ermöglicht werden. Ebenso sinnvoll im Ansatz, aber konkretisierungsbedürftig in der Ausführung sind die Regelungen zur Produktzertifizierung. Der Gesetzentwurf sieht nur die Zertifizierungspflicht bzw. eine Sicherheitsinspektion vor, legt aber keine exakten Qualitätsvorgaben für die Zertifizierungsstellen fest. Gerade für Datenschutz- und Datensicherheitszertifizierungen ist es von herausragender Bedeutung, dass nicht jedwede Institution derartige Gütesiegel vergeben kann und auch die Institution selbst regelmäßig auf die Einhaltung von Qualitätsstandards überprüft wird. Schon im deutschen Raum ist die Anzahl der Zertifizierungsstellen zu unübersichtlich.

An den Regelungen zur Gewährung des Netzwerkzugangs gibt es hingegen nichts auszusetzen. Positiv hervorzuheben ist ebenso die Einführung einer Meldepflicht für Netzwerkbetreiber gem. den Vorgaben eines eigenen Notfallplans. Dieser Notfallplan müsste von einer unabhängigen Stelle in regelmäßigen Abständen zusätzlich noch auf seine Gesetzeskonformität und Einhaltung hin überprüft werden. Gegen die Art. 23 und Art. 24 hingegen bestehen durchgreifende Bedenken: Die Zusammenarbeit mit den staatlichen Behörden zu Zwecken von u.a. strafrechtlichen Verfahren wird in keinster Weise konkretisiert und belässt erheblichen Spielraum zur Übermittlung und Auswertung von im Zweifelsfall großen Mengen personenbezogener Daten.

Der zweite Abschnitt des 3. Kapitels befasst sich im Speziellen mit dem Schutz von KRITIS, wobei die hier anzutreffende Legaldefinition inhaltlich von der zuvor beschriebenen abweicht, indem sie inhaltlich erweitert wird. Wie bereits angemerkt, ist der Schutz von KRITIS im Gesetzentwurf auf die Koordination durch einzelne Verwaltungseinheiten angelegt. Die „State Council departments“ sind individuell dazu aufgefordert, Schutzmaßnahmen einzuführen und zu überwachen. Ähnlich wie in Art. 17 sieht Art. 28 für den Schutz von KRITIS ebenso verschiedene Betreiberpflichten vor, die jedoch keiner Kontrolle unterliegen. Soweit kritische Infrastrukturen verwaltet werden, ist eine Verpflichtung der Betreiber vorgesehen, dabei entstehende personenbezogene Daten der Bürger in Festlandchina zu speichern. Anderenfalls ist eine Sicherheitsbewertung vorgesehen. Da Deutschland und die EU auf Grund ihres hohen Datenschutzstandards in jedem Falle als „sicheres Drittland“ zu qualifizieren sein dürften, sollten an dieser Stelle erleichterte Vorgaben geschaffen werden, um die Datenübermittlung zu ermöglichen, den Verwaltungsaufwand herabzusetzen und dadurch zu beschleunigen. Für Art. 33 Abs. 3 des Gesetzentwurfs sollte abschließend eine Konkretisierung des Begriffs „network security information“ stattfinden.

Zu Chapter 4: Network Information Security

Im vierten Kapitel des Gesetzentwurfs werden vornehmlich Vorschriften zum Schutz personenbezogener Daten der durch die Datenverarbeitung Betroffenen festgelegt. Eingangs sieht Art. 34 deshalb vor, dass die Betreiber Schutzsysteme vorsehen sollen, die insb. der individuellen Privatsphäre, aber auch dem Schutz von Wirtschaftsgeheimnissen Rechnung tragen sollen. Gleichwohl befassen sich die folgenden Vorschriften im Wesentlichen nur mit dem Schutz von personenbezogenen Daten, u.a. mittels einer Regelung, die dem Grundsatz der Datensparsamkeit nach deutschem Recht ähnlich ist sowie einer dem Zweckbindungsgrundsatz vergleichbaren Bestimmung.

Auffallend ist bei zahlreichen Vorschriften die Verwendung des Begriffs „citizen's personal information". Teils taucht diese Bezeichnung auch unter Bezugnahme auf bilaterale Abkommen auf. Deshalb stellt sich die Frage, wie weitgreifend diese Begrifflichkeit gewählt ist. Die in Art. 66 enthaltene Legaldefinition enthält nur Hinweise darauf, welche Datenkategorien erhoben werden sollen, jedoch nicht, welche Personengruppen genau unter „citizen" fallen. Hier sollte eine weitergehende Konkretisierung angestrebt werden. Die Informationsverpflichtung bei Datenlecks aus Art. 36 Abs. 2 ähnelt den Vorgaben des § 42a BDSG und ist aus diesem Grunde zu begrüßen. Gleichwohl sollten zusätzliche Regelungen vorgesehen werden, welche die Einhaltung dieser Informationsverpflichtung sicherstellen. Falls personenbezogene Daten deutscher oder europäischer Bürger betroffen sind, sollte ferner auch darüber nachgedacht werden, über eine deutsche bzw. europäische Kontaktstelle sicherzustellen, dass auch ausländische Behörden koordinierte Informationen über Art und Ausmaß des Datenlecks erhalten.

Art. 37 sieht ein Recht auf Löschung und Berichtigung personenbezogener Daten vor. Grds. kann ein solches Recht aber nur dann sinnvoll ausgeübt werden, wenn den Betroffenen einer Datenverarbeitung vorgängig das Recht eingeräumt wird, Auskunft über die Daten zu erhalten, die bei einem Verantwortlichen gespeichert sind. Dies entspricht auch nationalen und europäischen Regularien in diesem Bereich. Art. 43 ist nicht mit den europäischen Regelungen zur Informationsfreiheit vereinbar, da hierdurch im Ergebnis eine willkürliche Einschränkung des aus dem Ausland kommenden Datenverkehrs möglich ist.

Zu Chapter 5: Monitoring, Early-warning and Emergency Response

Art. 44 bestimmt Vorgaben zur zentral und einheitlich koordinierten Realisierung von Netzwerksicherheit. U.a. werden ein Frühwarn- und ein Informationssystem vorgeschlagen, das denen der nationalen europäischen CERTs ähnelt, deren neuerliche Vorgaben auch aus dem IT-SiG und der NIS-RL fließen. Die hierzu im Gesetzentwurf vorgeschlagenen Regelungen sind dementsprechend auch zu großen Teilen sinnvoll und notwendig, um ein hohes Maß an IT-Sicherheit zu garantieren. Art. 50 geht mit der Möglichkeit der Einschränkung des Netzwerkverkehrs in bestimmten Regionen über gegenwärtige europäische Regelungen hinaus. Es fehlen im Bereich der Überwachung der Netzwerksicherheit solche Regelungen, die sicherstellen, dass auch Einrichtungen oder Behörden über sie betreffende IT-Sicherheitsvorfälle und Bedrohungen gewarnt werden, die sich in einem Drittland befinden, mit welchem bilaterale Abkommen geschlossen wurden. Im Sinne einer gesamtheitlichen Koordinierung der Abwehr von IT-Sicherheitsrisiken könnte sich eine solche Vorschrift als besonders hilfreich für deutsche und europäische Behörden erweisen. Allgemein stellt sich die Frage, ob im Sinne einer verbesserten

transnationalen Zusammenarbeit spezielle Regelungen geschaffen werden sollten, die den Informationsfluss zwischen den europäischen und chinesischen Behörden im Bereich der IT- und Netzwerksicherheit verbessern, soweit die Einhaltung des Zweckbindungsgrundsatzes nachprüfbar ist.

Zu Chapter 6: Legal Responsibility

Entscheidend für die tatsächliche Umsetzung teils kostenintensiver organisatorischer Maßnahmen zur IT-Sicherheit seitens der Verantwortlichen und Betreiber ist die Schaffung geeigneter Anreize hierfür. Hier spielen insb. Ordnungswidrigkeiten eine nicht unerhebliche Rolle, indem IT-Verantwortlichen bei Zuwiderhandlungen Geldbußen angedroht werden. Dementsprechend sieht Kapitel 6 des Gesetzentwurfs solche Regelungen vor. Sinnvoll ist hierbei die Trennung der Verantwortlichkeiten zwischen dem Unternehmen als juristischer Person und den unmittelbar dafür verantwortlichen Personen, welche gleichermaßen mit Bußgeldzahlungen belegt werden können. Für KRITIS gelten erhöhte Summen. Ebenso vorgesehen ist, dass der Gewinn im Falle unrechtmäßiger Datennutzungen eingezogen werden kann. Wichtig ist vor allem auch die Regelung des Art. 52, mittels derer sichergestellt wird, dass Endprodukte- und Softwarehersteller ebenfalls eine Zahlungspflicht trifft, sollten sie z.B. Malware verbreiten. Gerade unter Gesichtspunkten des Exports und Imports sollte eine solche Vorschrift zwingend beibehalten werden.

Für alle Bußgeldvorschriften gilt, dass ihre Effektivität mit der behördlichen Kontrolldichte der durch den Gesetzentwurf benannten Maßnahmen steht und fällt. Ausreichende behördliche Personalkapazitäten zur Umsetzung müssen deshalb in jedem Falle vorgesehen werden, damit die gesetzlichen Vorgaben nicht letztlich nur zu einer theoretischen Wirksamkeit gelangen. Für sämtliche der in diesem Kapitel genannten Geldbeträge gilt, dass nicht beurteilt werden kann, ob ihre Höhe die nötige Abschreckungswirkung erreicht. Die Höhe der Bußgelder muss deshalb einer gesonderten Überprüfung zugeführt werden. Grds. sollten sich die Sätze im Mindesten an den Vorgaben orientieren, welche das deutsche und europäische Datenschutzrecht vorgibt.

Zu Chapter 7: Supplementary Provisions

Das siebte und letzte Kapitel des Gesetzentwurfs enthält Begriffsdefinitionen. Anzudenken wäre, eine zusätzliche Definition zum Schutz besonderer Arten von personenbezogenen Daten einzufügen, die bisher fehlt. Generell sollten für Daten wie Gesundheitsinformationen etc. besondere Arbeits- und Schutzkriterien vorgesehen werden.

Abschließende Stellungnahme

Der chinesische Gesetzentwurf zum Cybersecurity Law enthält wesentliche datenschutz- und datensicherheitsrechtliche Vorgaben, um die europäisch- bzw. deutsch-chinesische Zusammenarbeit zu stärken, für die möglichst angeglichene IT-sicherheitsrechtliche Vorstellungen notwendig sind, insb. auch für den Fall, dass Daten aus der EU nach China übermittelt werden. Gleichwohl bleiben die Regulierungsvorschläge des Cybersecurity Law in einigen Punkten hinter den europäischen Vorgaben zurück. Augenscheinlich ist dies in zahlreichen Fällen zunächst nicht schwerwiegend, in der Gesamtschau aber sollten die in der Stellungnahme angemerkten Punkte nach Möglichkeit umgesetzt werden, um einen möglichst hohen und in seiner Umsetzung effektiven IT-Sicherheitsstandard zu erzielen.

Weiterführende Links

Vgl. auch *Voigt*, ZD-Aktuell, 2015, 04759; *Schütze*, ZD-Aktuell, 2015, 04755 und zum Verbrauerschutz in China *Binding* ZD 2014, 327.