# Update zum *Cyber Security Law* in China

**Dr. Thomas Pattloch,**
LL.M Eur., Rechtsanwalt und Partner bei Taylor Wessing Partnerschafts-gesellschaft

Das *Cyber Security Law* und die mit diesem Gesetz einhergehenden Änderungen sorgen auch in 2018 für Unsicherheit und Besorgnis auf Seiten der deutschen Industrie und Forschung.

## 1. Rückblick

Das *Cyber Security Law* trat am 1. Juni 2017 in Kraft.[1] Zusammen mit der neuen *Cyberspace Administration of China* „CAC"[2] stellt es das Rückgrat einer neuen Vision des Internets durch die chinesische Führung dar. Netzsouveränität mit chinesischen Charakteristiken, Datenschutz und Kontrolle über Inhalt und Nutzer des Netzes sind wichtige Bestandteile dieser Vision, die in wirtschaftlicher Hinsicht ergänzt wird durch die sog. „Internet Plus Initiative"[3] aus dem Jahr 2015.

## 2. CIIO und besondere Verpflichtungen

Das *Cyber Security Law* stellt erhebliche organisatorische und rechtliche Anforderungen an verschiedene Nutzergruppen des Internets. Besonders intensiv reguliert werden die sog. Betreiber kritischer Informationsinfrastrukturen („*Critical Information Infrastructure Operators*" oder „CIIO")[4]. Sie müssen nicht nur unter anderem kontinuierliche, nachweisbare Vorkehrungen zum Cyberschutz treffen, regelmäßige Trainings der Mitarbeiter und eigener IT-Spezialisten abhalten sowie organisatorische Notfallpläne im Falle eines Hackerangriffs erstellen.[5] Noch wichtiger ist die Beschränkung für diese Art von Nutzern, personenbezogene Daten und sog. „wichtige Daten", welche in China erhoben oder gesammelt wurden, lokal in China zu speichern und nur unter engen Voraussetzungen ins Ausland zu transferieren.[6] Sie müssen vor einer Übertragung eine Sicherheitsüberprüfung durchlaufen, welche auch chinesische Regierungsstellen und externe Experten umfassen.[7]

Derzeit bestehen große Unsicherheiten, wer als ein CIIO anzusehen ist. Erste Entwürfe der zuständigen Agentur aus dem Jahr 2017 haben in den Umfang dieser Gruppe auch die wissenschaftliche Forschung und Produktion in den Industriebereichen Verteidigung, Wissenschaft und Industrie, große Industrieanlagen und Ausrüstungen, petrochemische Industrie, Nahrungsmittel und die pharmazeutische Industrie gefasst.[8] Zumindest in diesen Bereichen muss derzeit davon ausgegangen werden, dass ein Datenexport aus China heraus nicht ohne weiteres zulässig ist.

## 3. Pflichten der Netzwerkbetreiber

Immer noch unklar ist weiterhin, ob auch sogenannte einfache Netzwerkbetreiber („*Network Operators*") eine Pflicht haben, in China gewonnene Daten lokal zu speichern und vor einem Datenexport zwingend eine Sicherheitsüberprüfung entweder selbst oder durch zuständige Behörden durchführen zu müssen. Das *Cyber Security Law* selbst gibt hierzu keine eindeutigen Vorgaben.[9] Vielmehr finden sich Hinweise zu einer solchen Pflicht in mehreren Entwurfsfassungen von Verwaltungsanordnungen und Entwürfen zu technischen Standards zur Internetsicherheit mit unterschiedlichen Definitionen und Begriffen.[10] Die Pflichten insbesondere zu einer Sicherheitseinstufung vor einem Transfer werden hierbei teils ausdrücklich nicht nur auf CIIO erstreckt, sondern auch auf einfache Netzwerkbetreiber.

Die derzeit letzte Fassung des Entwurfs der Regelung des Datenexports beschränkt sich auf eine Umschreibung der Pflichten zur Sicherheitseinstufung auch für Netzwerkbetreiber, ohne die in früheren Entwürfen enthaltenen Verpflichtungen zur lokalen

[1] Englische Übersetzung z.B. unter: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
[2] www.cac.gov.cn
[3] http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm
[4] Vgl. Art. 31 *Cyber Security Law* und ff.
[5] Art. 34 *Cyber Security Law*.
[6] Art. 37 *Cyber Security Law*.
[7] Vgl. Art. 2 *Draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data*, 19 May 2017.
[8] Art. 18 CAC *Circular on Seeking Public Comments on the Regulations on the Protection of the Securityof Critical Information Infrastructure (Draft for Comment)*, 10 July 2017.
[9] Art. 37 *Cyber Security Law* spricht nur von "*Critical Information Infrastructure Operators*".
[10] Art. 2 *Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data* spricht von der Notwendigkeit, vor einem Transfer ins Ausland ein "*security assessment*" vornehmen zu müssen; die erste Fassung dieser Draft Measures vom 11. April 2017 formulierte ausdrücklich in Art. 2 die Pflicht für sämtliche Netzwerkbetreiber, Daten lokal speichern zu müssen. Der *Draft Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment* vom 25. August 2017 spricht bezüglich des Datentransfers ins Ausland in den Art. 3.7 und 3.9 von "Netzwerkbetreibern", nicht lediglich CIIO.

Datenspeicherung auch für Netzwerkbetreiber aufzuführen. Soweit aber eine Sicherheitsüberprüfung vor einem Datenexport durchzuführen ist und diese im Einzelfall dazu führen kann, dass ein Export aus Sicherheitsgründen nicht zulässig ist, entsteht de facto auch für diese Gruppe von Internetnutzern eine Pflicht zur (zumindest vorläufigen) lokalen Datenspeicherung.

## 4. Das System der Einstufung nach Sicherheitsgraden

Die Einstufung der Sicherheit von Netzwerken einschließlich ihrer personenbezogenen Daten und wichtigen Daten wird derzeit ebenfalls in einer Vielzahl von Entwürfen der jeweils zuständigen Behörden CAC, *Ministry of Public Security* (MPS), *Ministry of Industry and Information Technology* (MIIT) und anderen geregelt. Das System folgt hierbei dem fünfstufigen Aufbau des Multi-Level *Protection Scheme* des *Ministry of Public Security* für Netzwerke allgemein[11], und gibt seinerseits teils sehr strenge Kriterien vor.[12] Je höher die Sensibilität von Daten einzustellen ist, desto schneller wird eine Sicherheitsüberprüfung in Zusammenarbeit mit den chinesischen Behörden und Experten notwendig.[13] Dies wiederum erhöht die Wahrscheinlichkeit, dass bei Einstufung eines Netzwerks per se als „kritisch" ein Datenexport nicht ohne weiteres möglich sein wird. Es gibt in den derzeit gültigen Entwurfsfassungen keine festen Fristen, innerhalb derer die Einstufung und ggf. Erlaubnis der Behörden abgeschlossen sein müssen, wohl aber Fristen zur Registrierung bei den zuständigen Behörden.

## 5. Das Verfahren der Sicherheitseinstufung und Pflichten für Netzwerkbetreiber

Für internationale Forschungsvorhaben relevant ist das am 27. Juni 2018 durch das MPS verkündete *Announcement of the Ministry of Public Security on Seeking Public Comments on the Regulations on the Graded Protection of Cyber Security (Draft for Comment)*. Die *Draft Regulations* gelten für sämtliche Netzwerkbetreiber und Internetnutzer mit Ausnahme des privaten Bereichs.[14] Die darin festgelegte Sicherheitsüberprüfung anhand dieser *Draft Regulations* folgt einem sehr detailliert festgelegten Verfahren.

Zuerst muss durch das betroffene Unternehmen, die Forschungseinrichtung oder das Individuum eine Art Sicherheitseinstufung erstellt werden zur Registrierung bei den Behörden[15]. In Art. 6 dieses Entwurfs wird erneut die Notwendigkeit auch für bloße Netzwerkbetreiber betont, eine Sicherheitsüberprüfung selbst durchzuführen und diese mit den chinesischen Behörden bzw. der Polizei zu registrieren. Der Entwurf regelt weiter ausführlich die Einstufung in die fünf Grade anhand offener Begriffe wie „*will lead to [harm/serious harm/extremely serious harm] to the lawful rights and interests of related citizens, legal persons and other organiz*ations".

Die Einstufung muss demnach anhand der Kriterien in nationalen Standards überprüft werden, ob eine Störung des Netzwerks private Rechte und Interessen von „Bürgern", die öffentliche Ordnung oder das öffentliche Interesse und schließlich die nationale Sicherheit betroffen wären. Der Entwurf (und damit im Zusammenhang stehende Standards) enthalten hierbei lediglich Eckpunkte und nicht weiter definierte Begriffe, die zur Beurteilung des Risikograde heranzuziehen sind, während weitere Einzelheiten in nationalen Standards bzw. „*Guiding Opinions*" ausformuliert werden sollen.[16]

Die Einstufung ist sehr bedeutsam, da gem. Art. 17 des Entwurfs schon ab Grade II ein *Review* durch ein Expertengremium erforderlich ist zusammen mit einer Anmeldung bei der Polizei innerhalb einer zehn Tages Frist, Art. 18. Ohne dies darf ein Netzwerksystem nicht betrieben werden, Art. 22 Entwurf.

Die Überprüfung ist jährlich erneut durchzuführen, Art. 25 Entwurf. Internetsysteme ab Grade III müssen grundsätzlich innerhalb Chinas gehostet und gewartet werden, vgl. Art. 29 Entwurf.[17]

---

[11] *Draft Regulations on Cyber Security Multi-Level Protection Scheme*, veröffentlicht durch MPS am 27. Juni 2018. In China basierte Informationssystem im Internet ab Level 3 sind erhöhten Anforderungen unterworfen. Damit im Zusammenhang steht der Information *Security Technology-Guidelines for Grading of Cybersecurity Multi-Level Protection Standard*, veröffentlicht durch das *National Information Security Standardization Technical Committee* am 19. Januar 2018.

[12] vgl. *Announcement of the Ministry of Public Security on Seeking Public Comments on the Regulations on the Graded Protection of Cyber Security (Draft for Comment): Article 15 [Cyber Grades] Cyberspace is graded at five different levels for security protection purposes, depending on the importance of the cyberspace in national security, economic construction and social life, the extent of harm caused to the national security, public order, public interests and the lawful rights and interests of related citizens, legal persons and other organizations when the cyberspace is disrupted or malfunctions or the data is falsified, divulged, lost or destroyed, and other relevant factors.*
*1. Grade I cyberspace refers to ordinary networks, the disruption of which will lead to harm to the lawful rights and interests of related citizens, legal persons and other organizations, but will not undermine the national security, public order and public interests;*
*2. Grade II cyberspace refers to ordinary networks, the disruption of which will lead to serious harm to the lawful rights and interests of related citizens, or harm to the public order and public interests, but will not undermine the national security;*
*3. Grade III cyberspace refers to important networks, the disruption of which will lead to extremely serious harm to the lawful rights and interests of related citizens, or serious harm to the public order and public interests, or harm to the national security;*
*4. Grade IV cyberspace refers to particularly important networks, the disruption of which will lead to extremely serious harm to the public order and public interests, or serious harm to the national security; and*
*5. Grade V cyberspace refers to extremely important networks, the disruption of which will lead to particularly serious harm to the national security.*

[13] Ab Level 3 gemäß der *Draft Regulations on Cyber Security Multi-Level Protection Scheme*, und hiervon abweichend schon ab *Grade* II gemäß Art. 17 der *Regulations on the Graded Protection of Cyber Security (Draft for Comments)*, veröffentlicht durch das MPS am 27. Juni 2018.

[14] Art. 2 *Regulations on the Graded Protection of Cyber Security (Draft for Comments): "These Regulations shall apply to the construction, operation, maintenance and use of cyberspace, the graded* protection of cyber security, *as well as the supervision and administration of such protection, within the territory of the People's Republic of China. The said cyberspace excludes networks set up by individuals and families themselves for personal use*."

[15] Art. 6, 16, 18 *Regulations on the Graded Protection of Cyber Security (Draft for Comments)* mit einer Frist von zehn Tagen nach Abschluss der Einstufung und Ausstellung eines „*Record Filing Certificate*", Art. 19.

[16] Art. 9, 17 Abs. 3 *Regulations on the Graded Protection of Cyber Security (Draft for Comments).*

[17] Art. 29 *[Technical Maintenance Requirements] Cyberspace at or above Grade III shall be technically maintained within the territory of China, and remote technical maintenance from overseas is prohibited. Where it is truly necessary to have cyberspace technically maintained remotely from overseas due to business needs, it is required to assess the cyber security and take necessary measures to manage and control risks. Technical maintenance shall be recorded and the technical maintenance logs shall be safekept and provided when the public security organ performs inspections.*

Auch die Tätigkeit im Internet wird bezüglich Datensammlung auf das chinesische Konzept des erlaubten „*business scope*" beschränkt, Art. 31 Abs. 2 Entwurf[18]:
Der Entwurf verweist schließlich für die Sanktionen im Wesentlichen auf das *Cyber Security Law*, führt aber auch ein persönliches Interrogationsrecht von gesetzlichen Vertretern von Unternehmen und den benannten IT-Verantwortlichen ein, vgl. Art. 62 Entwurf.[19]

Die teils sehr weitgehenden Anforderung an die Beurteilung der Auswirkungen eines Datenexports werden es im Zweifelsfall Dateninhabern 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.

## 6. Forschung in China

Für Forschungsvorhaben in China bedeuten die jüngsten Entwürfe eine deutliche Erschwerung der Rahmenbedingungen, da vorab eine Dateninterpretation nicht nur durch die Forschenden selbst vorgenommen werden muss, sondern auch den Behörden (und ggf. Dritten als Teilen der Expertenkommission) erklärt werden muss. Dies führt zu einer weitgehenden Offenbarung der Zielrichtung und des wissenschaftlichen und wirtschaftlichen Werts der erforschten Daten, aber auch zu einem erheblichen Begründungs- und Mehraufwand. Auch besteht ein Risiko im Hinblick auf die Sinnhaftigkeit eines Forschungsprojekts, wenn die Daten nicht exportiert werden können bzw. die Anforderungen einer Sicherheitseinstufung in Grade III beispielsweise mit lokaler „*data maintenance*" nicht erfüllt werden können. Ein effektiver Geheimhaltungsschutz schließlich kann durch die chinesischen Behörden rein faktisch nicht gewährleistet werden, da spätestens im Falle der Einschaltung Dritter als Experten die Weitergabe von Informationen nicht kontrolliert werden kann.

Ein weiteres praktisches Problem am derzeitigen System stellt die potentielle Masse an Antragstellern zur Bestätigung der Sicherheitseinstufung dar. Es ist angesichts der Größe der CAC, der personellen Ausstattung der MPS und der Vielzahl an Forschungsprojekten in China kaum vorstellbar, wie eine objektiv nachvollziehbare und sinnvolle Prüfung in einem machbaren Zeitrahmen stattfinden kann. Da in jedem Fall der substantiellen Änderung des Datenflusses oder der Datenqualität auch immer wieder eine erneute Sicherheitseinschätzung erforderlich wird[20], würden auch Änderungen z.B. des Subjekts der Datenerhebung oder des Forschungsbereichs jedes Mal potentiell zu erneuten Verzögerungen führen. An der bisherigen Konstruktion des Gesetzes zeigt sich ein umfassender Kontrollanspruch, welcher de facto mit Durchführung des Gesetzes je nach Ermessen der chinesischen Seite abgeschwächt oder gar nicht ausgeübt werden könnte, aber andererseits auch jederzeit in Gang gesetzt werden kann.

Als ein Lichtblick muss deshalb gelten, dass wesentliche Bestandteile des neuen Systems noch nicht durch die zuständigen Behörden und Ministerien entschieden worden sind und immer noch im Entwurfsstadium diskutiert werden. Offiziell war von chinesischer Seite bis Ende 2018 eine Gnadenfrist für betroffene Unternehmen und Individuen eingeräumt worden. Seit Juni 2017 wurde auch eine Fülle von weiteren Standards, Verwaltungsanordnungen und Entwürfen zur Konsultation veröffentlicht, zuletzt am 15. September 2018 die *Ministry of Public Security Provisions on the Supervision and Inspection of Internet Security by Public Security Organs*, welche vor allem die Eingriffs- und Überwachungsrechte der Polizei einschließlich Fernzugriffe beinhalten.

Zusammengefasst zeigen die jüngsten Entwürfe immer noch eine Gestaltung des Rechtsrahmens mit Betonung auf maximaler Kontrolle. Es finden sich kaum Erleichterungen oder Ausnahmen z.B. von gemeinnütziger Wissenschaft und Forschung von den strengen Vorgaben des neuen Rechtsrahmens. Das typisch chinesische System der „Selbstkontrolle" mit anschließender Registrierung und jederzeitiger staatlicher Kontrolle wird bislang ohne Rücksicht auf die Interessen anderer Bereiche durchgesetzt und vorgeschrieben.

Hierbei hilft nicht, dass die im *Cyber Security Law* verankerten Sanktionen maßvoll sind. Die Gefahr, durch die Behörden ausgespäht oder „aufs Korn genommen" zu werden, ist im Gesetzesrahmen angelegt. Internationale Forschungsvorhaben müssen daher in Zukunft genauso wie Rüstungsunternehmen oder die pharmazeutisch-medizinische Industrie hohe Anforderungen an die Eigenorganisation der IT und Datenflüsse leisten. Es bleibt zu hoffen, dass die letztendlich noch zu erlassenden Verwaltungsanordnungen diesen Trend abschwächen werden.

[18] "*Without permission or authorization, no cyber operator shall collect any data and personal information unrelated to the services it offers, collect, use or process any data and personal information in violation of the provisions of laws and administrative regulations or contrary to the agreement reached with users, divulge, falsify or destroy the data and personal information it has collected, or access, use or provide data and personal information without authorization.*"

[19] Art. 62 *[Interview System for Cyber Security] The public security organ, the secrecy administration and the cryptogram administration of the people's governments at or above the provincial level may hold an interview with the legal representatives and heads of cyber operators and the competent authority of the concerned industry, upon discovery of relatively major hidden security risks on the network or occurrence of cyber security events, while they are fulfilling their supervisory and administrative duties in the graded protection of cyber security.*

[20] Vgl. Art. 16 Abs. 2 *Regulations on the Graded Protection of Cyber Security (Draft for Comments).*