Unternehmerische IT-Compliance in China: Cybersecurity und Künstliche Intelligenz

Dennis-Kenji Kipker

A. Einführung

Wirtschaftsbeziehungen machen nicht an Landesgrenzen halt – ebenso wenig die transnationalen Datenströme. Ganz im Gegenteil: Wo einerseits weltwirtschaftlich immer mehr an Vernetzung stattfindet, so spiegelt sich diese denknotwendigerweise auch im internationalen und digitalen Informationsaustausch wider. Dabei ist der Informationsaustausch aber mit nicht unerheblichen Risiken für die Cybersicherheit verbunden, und so werden nicht nur der deutsche und der europäische Gesetzgeber tätig, um den zunehmend gefährdeten Cyberraum abzusichern, sondern ebenso die Rechtssetzungsorgane anderer Staaten weltweit. Dies bedeutet folglich auch, dass international tätige Unternehmen – gleichgültig, ob Großkonzern oder KMU – sich im Rahmen ihrer IT-Compliance nicht nur darauf beschränken können, die gesetzlichen Regelungen ihres jeweiligen Herkunftslandes zu beachten, sondern sich genauso auf die Vielzahl an neuen Rechtsvorschriften in der Cybersicherheit einstellen müssen, die aktuell weltweit verabschiedet werden. Das ist nicht selten aufgrund der kulturellen, aber auch der sprachlichen Barrieren, eine erhebliche Herausforderung. Der vorliegende Beitrag widmet sich im Speziellen der Cybersicherheitsgesetzgebung in der Volksrepublik China, und hier mit einem Schwerpunkt auf dem Thema der Künstlichen Intelligenz (KI) als einer Schlüsseltechnologie, die nicht nur für die Cybersicherheit, sondern auch für die globale politische und wirtschaftliche Entwicklung des nächsten Jahrzehnts eine herausragende Relevanz besitzt.*

* Eine Aufzeichnung des Vortrags, auf dem der Beitrag beruht, ist abrufbar unter https://doi.org/10.17176/20210315-161623-0.

B. Regelungssystematik und politische Strategien

Mit einem Blick auf die rechtliche Entwicklung der Cybersicherheit in China wird recht schnell deutlich: China besitzt schon seit Jahrzehnten eine mehrschichtige Gesetzgebung zur IT-Sicherheit, und dürfte auf diesem Feld damit zu den globalen Vorreitern zählen. Das erste IT-sicherheitsrelevante Gesetz, die „Computer Information System Security Protection Regulations of the People's Republic of China", wurde in der Volksrepublik schon 1994 verabschiedet. In den letzten Jahren ist die chinesische IT-Sicherheitsgesetzgebung auch in westlichen Staaten immer wieder in den Fokus der öffentlichen Wahrnehmung gelangt. Das ist vor allem auf die Tatsache zurückzuführen, dass eine Vielzahl westlicher Unternehmen geschäftliche Niederlassungen in China betreibt, die dementsprechend von der neuen chinesischen Gesetzgebung zur IT-Sicherheit betroffen sind. Erschwerend hinzu tritt die unübersichtliche Behörden- und Zuständigkeitsstruktur auf mehreren Verwaltungsebenen sowie die Tatsache, dass viele Gesetze eher generalklauselartig formuliert sind und so weite begriffliche Interpretationsspielräume in ihrer konkreten Anwendung bestehen lassen.

Ein eigenständiges KI-Gesetz, das die IT-Sicherheit umfassend aufgreift und reguliert, existiert in China gegenwärtig dennoch nicht. Gleichwohl enthalten verschiedene andere chinesische Gesetze durch die Regulierung von technisch-organisatorischen Einsatzszenarien Bezugspunkte zur KI und zu möglichen (zukünftigen) Anwendungsfeldern, die sich hieraus entwickeln können. Trotz noch fehlender bereichsspezifischer KI-Gesetzgebung zur IT-Sicherheit bedeutet dies nicht, dass die Volksrepublik im Bereich der allgemeinen KI-Gesetzgebung nicht schon umfassend tätig ist.[1] Die Relevanz, die Peking dem Thema KI beimisst, wird außerdem durch die Strategie des Staatsrats deutlich, bis zum Jahr 2025 die weltweite Führungsposition bei KI zu übernehmen, und bis zum Jahr 2030 die weltweite Vormachtstellung zu erlangen, sowohl politisch wie auch wirtschaftlich.[2] Außerdem benennt der „Next Generation Artificial Intelligence Development Plan" (AIDP) aus Juli 2017 KI als eine zentrale Maßnahme zur Förderung der nationalen, wirtschaftlichen und sozialen Sicherheit von

1 Weiterführend dazu Roberts *et al.*, The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation, AI & Society 2020, https://doi.org/10.1007/s00146-020-00992-2 (abgerufen am 05.10.2020).

2 Konrad Adenauer Stiftung (Hrsg.), Vergleich nationaler Strategien zur Förderung von Künstlicher Intelligenz – Teil 1, 2018, S. 18 ff. mwN., so auch *Roberts et al.* (Fn.), ausdrücklich Bezug nehmend auf den Zehnjahresplan „Made in China 2025".

China.[3] In dem Dokument wird auf Sicherheitsaspekte von KI-Entwicklung nicht unter dem Aspekt der „Security", sondern auf die „Safety" verwiesen. Die Gefahren bei der KI-Nutzung werden folglich vorrangig nicht im Schutz des KI-Systems vor dem Menschen, sondern im Schutz des Menschen bzw. der durch ihn betriebenen Einrichtungen vor einer fehlgeleiteten KI und den dadurch eintretenden Schäden gesehen. Die IT-Sicherheit als solche rückt bei der gesetzgeberischen Betrachtung somit (zurzeit noch) in den Hintergrund.

Im Folgenden werden drei zentrale und aktuelle gesetzgeberische Maßnahmen zur IT-Sicherheit in China in einem Überblick vorgestellt: das Chinese Cybersecurity Law (CSL) aus 2016, das New Chinese Cryptography Law aus 2019 und das Chinese Data Security Law (DSL), das gegenwärtig noch in einer Entwurfsfassung aus 2020 vorliegt. Relevant ist unter Gesichtspunkten der Datensicherheit daneben das Personal Information Protection Law, das sich ebenfalls noch im Gesetzgebungsverfahren befindet. Wichtig ist, dass die chinesischen Rechtsgrundlagen zur IT- und Datensicherheit stets im Zusammenhang betrachtet werden, da sich die Regulierungsbereiche von einzelnen Gesetzen durchaus überschneiden können.

C. Chinese Cybersecurity Law

Das 2016 verabschiedete und im Juni 2017 in Kraft getretene CSL enthält sowohl Vorschriften zur IT-Sicherheit als auch zum Datenschutz – womit es eine der ersten gesetzlichen Regelungen in China gewesen ist, die explizit datenschutzrechtliche Anforderungen adressierte.[4] Hierzulande gelangte das Gesetz durch die Themen Regulierung von VPN-Verbindungen, Produktzulassung und Datenlokalisierung in das Blickfeld der öffentlichen Wahrnehmung zahlreicher Wirtschaftsunternehmen.[5] Als Hauptziele des CSL beschrieben werden die Sicherstellung der Netzwerksicherheit (im

3 China Association for International Science and Technology Cooperation, Next Generation Artificial Intelligence Development Plan Issued by State Council, http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf (abgerufen am 01.10.2020).

4 Zur Analyse der Entwurfsfassung des CSL aus 2015 siehe *Kipker*, MMR-Aktuell 2015, 370972, hierzu aktuell weiterführend *Chen/Han/Kipker*, An Introduction into the New Chinese Data Protection Legal Framework, DuD 2020, 52.

5 Vgl. *Kipker*, Chinese Cybersecurity Law: Neue rechtliche Wege und Umwege nach China, Tagungsband des BSI-Kongresses 2019, S. 475.

Wesentlichen gleichzusetzen mit der IT-Sicherheit), die Aufrechterhaltung der Souveränität im Cyberspace, der Schutz der nationalen Sicherheit und des öffentlichen Interesses, der Schutz der Rechte und Interessen von Bürgern, Rechtspersonen und sonstigen Einrichtungen, und eine Förderung der wirtschaftlichen und sozialen Entwicklung der Gesellschaft. Insbesondere die Kapitel 2 „Support and Promotion of Network Security", 3 „Network Operations Security" und 5 „Monitoring, Early Warnings, and Emergency Responses" enthalten zentrale Vorgaben zur IT-Sicherheit. Auf KI wird dabei jedoch nicht unmittelbar Bezug genommen, jedoch lässt sich über folgende Vorschriften des Gesetzes ein KI-Bezug herstellen:

- Art. 5: Der Staat hat die Aufgabe, IT-Sicherheitsrisiken zu überwachen und ihnen vorzubeugen, kritische Infrastrukturen zu schützen und rechtswidrige bzw. kriminelle Netzwerkaktivitäten zu erkennen, und auf diese Weise die Sicherheit und Ordnung im Cyberspace zu gewährleisten.
- Art. 7: Der Staat beteiligt sich an internationalem Austausch und Kooperation in der Entwicklung und Nutzung von Netzwerktechnologien, und formuliert entsprechende Standards.
- Art. 10: Es sind Maßnahmen vorzuhalten, die die Netzwerksicherheit und operationelle Stabilität des Netzwerks gewährleisten, und Maßnahmen umzusetzen, die effektiv auf Sicherheitsvorfälle reagieren, und Cyberkriminalität vorbeugen.
- Art. 15: Der Staat begründet, unterhält und verbessert ein System von Netzwerksicherheitsstandards.
- Art. 18: Der Staat fördert die Entwicklung von IT-Sicherheitstechnologien, und unterstützt innovative Maßnahmen zur Netzwerksicherheit. Hierzu können auch neue Netzwerktechnologien eingesetzt werden.
- Art. 21: Ein System der Netzwerksicherheit ist zu etablieren, das entsprechende technische Maßnahmen zum Schutz vor Computerviren, Netzwerkangriffen, und sonstigen schädlichen Eingriffen enthält. Die Maßnahmen umfassen ebenfalls die Überwachung und Aufzeichnung des Netzwerkstatus und von IT-Sicherheitsvorfällen.
- Art. 51: Der Staat richtet Systeme zur Netzwerküberwachung ein, sowie zu Frühwarnungen.

Auf der Grundlage des CSL wurden und werden überdies verschiedene untergesetzliche Regelwerke sowie technische Normen und Standards verfasst, bzw. sind in Bearbeitung, die ebenfalls ein Einfallstor für KI und

IT-Sicherheit bilden.[6] Hier dürfte in den kommenden Jahren am ehesten eine weitere konkrete Ausgestaltung des CSL zu verorten sein. Auffällig ist dabei aber, dass IT-Sicherheit in Bezug auf KI gegenwärtig nicht zu den Schlüsseltechnologien gezählt wird, die Entwicklung ist hier vielmehr noch allgemeiner gehalten bzw. bezieht sich auf andere Anwendungsfelder, so werden genannt: Machine Learning, knowledge graphs, natural language processing, human-computer interaction, computer vision, biometric feature recognition und virtual reality/augmented reality – in dem Zusammenhang wird jedoch der Ausblick gegeben, dass die chinesische KI-Entwicklung zukünftig nicht von bereichsspezifischen, sondern von allgemeinen Anwendungsfeldern ausgeht, die eine Vielfalt möglicher Einsatzszenarien abdecken, sodass hiervon zwangsläufig auch IT-Sicherheit umfasst ist.[7]

D. Chinese Cryptography Law

Das neue chinesische Kryptografiegesetz wurde im Oktober 2019 verabschiedet und trat zum 1.1.2020 in Kraft (vgl. Art. 44 des Gesetzes).[8] Ziel des Gesetzes ist die Entwicklung neuer kryptografischer Verfahren, Dienste und Produkte in China, womit auch die Stärkung der IT-Sicherheit einhergeht – explizit wird dies in Art. 1 des Gesetzes hervorgehoben. Die IT-Sicherheit steht dabei im Fokus der öffentlichen und nationalen Sicherheitsinteressen Chinas.[9] Insoweit bestehen von der rechtspolitischen Zielsetzung deutliche Parallelen zum CSL. Auch das Kryptografiegesetz enthält aber keine ausdrückliche Bezugnahme auf KI, sodass auch hier der Bezug mittelbar durch die Auslegung des Gesetzes herzustellen ist. Dies ist aufgrund der generalklauselartigen Formulierung vieler chinesischer Rechtsvorschriften aber nicht unbedingt als Hinweis dahingehend zu in-

6 Im Überblick dazu *Kipker/Scholz*, Cybersicherheit und Datenschutz in China – TC 260 stellt neue Normungsentwürfe vor, DuD 2018, 768.

7 China Electronics Standardization Institute (CESI)/Standardization Administration of China (SAC), Artificial Intelligence Standardization White Paper (2018 Edition), S. 20 f., http://www.cesi.cn/images/editor/20180124/20180124135528742.pdf (abgerufen am 01.10.2020).

8 Für die vollständige englische Sprachfassung des Cryptography Law of the People's Republic of China: https://www.chinalawtranslate.com/en/cryptography-law/ (abgerufen am 01.10.2020).

9 Zum Entwurf und zur rechtspolitischen Debatte zum chinesischen Kryptografiegesetz siehe *Kipker/Scholz*, China: Neue Vorgaben zur Cybersicherheit – Entwurf des Kryptografiegesetzes veröffentlicht, MMR-Aktuell 2019, 419468.

terpretieren, dass das Gesetz eine KI-Regulierung ausschließt. Wie auch für das EU-Recht erweist sich die Technologieoffenheit des chinesischen Rechts insoweit als signifikanter Vorteil, wenn es um Flexibilität und Anpassungsoffenheit im Hinblick auf die Einbindung neuer Technologien geht.

Systematisch untergliedert sich das Chinese Cryptography Law in die fünf Kapitel „General Provisions", „Core Cryptography, Common Cryptography", „Commercial Cryptography", „Legal Responsibility" und „Supplementary Provisions". Den Kern der Regelungen bildet die Unterscheidung zwischen verschiedenen kryptografischen Verfahren, an die stufenmäßig unterschiedliche Nutzungsanforderungen angelegt werden: „Core Cryptography", „Common Cryptography" sowie „Commercial Cryptography". Die beiden erstgenannten Verfahren sollen zum Schutz von Staatsgeheimnissen eingesetzt werden, demgemäß unterfallen sie als Staatsgeheimnis selbst einem entsprechenden Schutz. Die drittgenannte Kategorie kryptografischer Verfahren, die „Commercial Cryptography", wird für den Schutz jeglicher Information herangezogen, die kein Staatsgeheimnis ist – im Umkehrschluss ist sie somit zur Verschlüsselung sämtlicher herkömmlicher Daten nutzbar, um die IT-Sicherheit von Unternehmen und Privatpersonen zu gewährleisten. Insbesondere bei der Entwicklung und Anwendung kryptografischer Verfahren ist sicherzustellen, dass diese informationstechnisch nicht kompromittiert werden, vgl. Art 17 (für „Core Cryptography" und „Common Cryptography") und Art. 24 (für „Commercial Cryptography") des chinesischen Kryptografiegesetzes. Ein direkter Bezug zum CSL ergibt sich für die Überprüfung kryptografischer Produkte überdies aus Art. 26 und Art. 27 des Kryptografiegesetzes.

E. Chinese Data Security Law

Die hohe Bedeutung, die die chinesische Regierung der IT- und Datensicherheit bemisst, wird durch das umfängliche gesetzgeberische Tätigwerden der vergangenen Jahre besonders deutlich. So wurde Anfang Juli 2020 der Entwurf für ein neues chinesisches Datensicherheitsgesetz (Data Security Law, DSL) vom Standing Committee of the National People's Congress (NPC) veröffentlicht, der bis zum 16. August 2020 zu öffentlichen

Kommentierung zur Verfügung stand.[10] Das Gesetz betrifft die Datenverarbeitungsaktivitäten in Mainland China (vgl. Art. 2). Da es sich bei dem veröffentlichten Entwurf um eine frühe erste Entwurfsfassung handelt, ist im weiteren Verlauf des Gesetzgebungsverfahrens noch mit Änderungen zu rechnen. Das DSL wird systematisch als gleichrangige Regelung neben dem CSL stehen, und regelt über die IT- und Datensicherheit hinaus in erster Linie den Umgang mit Daten als Wirtschaftsgut, die Modalitäten von Datenverarbeitungsvorgängen, die Regelung von Zugriffsmöglichkeiten, und Möglichkeiten zu Open Data. Der Entwurf des Gesetzes untergliedert sich in insgesamt sieben Kapitel, die vom Allgemeinen zum Speziellen hin aufgebaut sind. Unter KI- und IT-Sicherheitsgesichtspunkten relevant sind das Kapitel 2 („Data Security and Development"), das Kapitel 3 („Data Security Systems"), das Kapitel 4 („Data Security Protection Responsibilities") und das Kapitel 5 („Government Data Security and Openness"). Folgende Vorschriften des Gesetzentwurfs sind im Einzelnen auch unter Gesichtspunkten von KI-Entwicklung besonders hervorzuheben:

- Art. 12: Der Staat ergreift Maßnahmen, um einerseits die Datensicherheit zu befördern, andererseits aber auch die Datennutzung zu ermöglichen. IT-Sicherheit wird als zentrales Kriterium der industriellen Entwicklung in China genannt.
- Art. 13: Der Staat verabschiedet eine Big Data-Strategie. Zur Datennutzung im Rahmen von Big Data sind innovative Technologien notwendig, wie beispielsweise sichere KI-gestützte Methoden der Datenauswertung.
- Art. 14: Der Staat fördert die wissenschaftliche Forschung im Bereich der Datenentwicklung und Datennutzung. Dabei wird ebenfalls die Datensicherheit genannt. In diesem Zusammenhang ist Art. 18 des Gesetzes zu sehen, der vorschreibt, dass der Staat personelle Ressourcen zur Datennutzung und Datensicherheit entwickelt.
- Ein Kernelement des DSL sind die Vorgaben in den Art. 19 ff. (Kapitel 3: „Data Security Systems"). Demnach werden die Datenbestände in unterschiedliche Schutzklassen unterteilt, jeweils in Abhängigkeit der Bedeutung für die wirtschaftliche und soziale Entwicklung, und gemessen an den Auswirkungen auf die nationale Sicherheit, das öffentliche Interesse und die Rechtsordnung. Hierzu baut der Staat u. a. ein zentralisiertes System der Risikoüberwachung auf, das ebenfalls ein Früh-

10 Data Security Law of the People's Republic of China (draft version), https://npcobserver.files.wordpress.com/2020/07/data-security-law-draft.pdf (abgerufen am 01.10.2020).

warnsystem enthalten kann – ein klassisches Einfallstor für KI in der IT-Sicherheit (vgl. Art. 20). Basierend auf detektierten Sicherheitsvorfällen sind die staatlichen Einrichtungen befugt, im Rahmen eines Notfallmanagements entsprechende Gegenmaßnahmen zu ergreifen (Art. 21).

- Art. 25: In dieser Bestimmung wird festgelegt, dass für die Datenverarbeitung Verantwortliche ein compliancegerechtes Management zur Datensicherheit etablieren müssen, das sich auf den gesamten Arbeitsablauf der Organisation erstreckt. Entsprechende technische Maßnahmen zur Datensicherheit müssen etabliert werden. Solche technischen Maßnahmen können letztlich auch KI umfassen.
- Art. 27: Soweit Daten verarbeitet werden, sollte eine Risikoüberwachung etabliert werden, die auch die IT- bzw. Datensicherheit betrifft. Eine solche Risikoüberwachung kann KI-gesteuert erfolgen.
- Art. 36: Staatliche Einrichtungen, die Daten verarbeiten, müssen ein Management zur Datensicherheit implementieren. Art. 37 DSL bestimmt weitergehend, dass sich staatliche Einrichtungen ihrer Pflicht zur Datensicherheit nicht dadurch entledigen können, indem sie die Datenverarbeitung an Dritte auslagern. Die Einhaltung entsprechender technisch-organisatorischer Maßnahmen ist weiterhin zu überwachen.
- Art. 41: Die IT- und Datensicherheit ist in einem fortlaufenden Prozess sicherzustellen – dies gilt sowohl für Aufsichtsbehörden als auch für datenverarbeitende Stellen.

F. Fazit und Ausblick

Bei einem Blick auf die chinesische Cyber-Sicherheitsgesetzgebung wird schnell deutlich, dass es nicht um ein einzelnes Gesetz geht, sondern eine Vielzahl unterschiedlichster Rechtsquellen, aber auch untergesetzliche Regelwerke sowie außerhalb des Rechts liegende technische Normen und Standards ausschlaggebend sind, um den regulatorischen Rahmen des Themas in China zu bestimmen. Das Zusammenspiel dieser unterschiedlichen Erkenntnisquellen mit jeweils verschiedener Granularität und Ansprüchen, aber auch das Fehlen einer transparenten und zentralisierten Kommunikationsstruktur erschwert den Umgang mit Compliance-Anforderungen zur Cybersecurity für Unternehmen in China enorm. Hinzu tritt, dass für weite Bereiche der chinesischen Cybersicherheitsgesetzgebung die Konkretisierung durch untergesetzliche Rechtsvorschriften und technische Normen und Standards noch nicht vollständig abgeschlossen ist bzw. zurzeit noch fortdauert und das Ende dieser Übergangsphase zur-

zeit nicht absehbar ist. Ausländische Unternehmen stehen hier aufgrund der undurchsichtigen chinesischen Behördenstruktur außerdem vor dem Problem, geeignete Ansprechpartner zu finden. Und selbst wenn ein solcher gefunden sein sollte, ist unklar, ob dieser eine rechtsverbindliche Auskunft erteilen kann oder darf. Kompetenzkonflikte zwischen den unterschiedlichen zuständigen Behörden und die sprachliche sowie kulturelle Barriere verschärfen diese Problematik. Die unklare Gesetzeslage tangiert dabei nicht nur betroffene Unternehmen selbst, sondern auch rechtsberatende Einrichtungen, die im Ausland tätig sind, weshalb verlässlicher und hinreichend verbindlicher (rechtssicherer) juristischer Rat im Hinblick auf das chinesische Recht der Cybersicherheit nicht leicht zu finden ist.

Angesichts der zahlreichen Unklarheiten von gesetzgeberischer Seite bleibt deshalb zumindest vorerst nur der Weg, die Implementierung der chinesischen Rechtsvorschriften zur Cybersicherheit weitestgehend über Best Practices voranzutreiben, die vor allem auch durch mittelständische deutsche Unternehmen entwickelt werden, die auf dem chinesischen Markt tätig sind. Nicht selten haben diese aufgrund jahrelanger Erfahrungen mit chinesischen Behörden und Providern einen Erfahrungsschatz gesammelt, der zwar keine klassische „Rechtssicherheit", wie wir sie hierzulande kennen, vermittelt, aber doch bei der Einschätzung, Kalkulierbarkeit und Prognose der rechtspolitischen Entwicklung und des behördlichen Handelns in China unterstützt. Zudem verfügen entsprechende Firmen zumeist über die notwendigen Kontakte zu Behörden und Geschäftspartnern, die essenzielle Voraussetzung für eine erfolgreiche unternehmerische Tätigkeit auf dem chinesischen Markt sind. Hier ist es wünschenswert, unter den betroffenen deutschen Unternehmen ein entsprechendes nationales Netzwerk für den Informations- und Erfahrungsaustausch zu etablieren. Soweit es die Kommunikation mit den chinesischen Behörden anbelangt, bleibt zu hoffen, dass auf absehbare Zeit konsolidierte Kommunikationskanäle und zentrale Ansprechstellen geschaffen werden, die bei der Beantwortung wesentlicher Fragestellungen zur Implementierung der Vorgaben des chinesischen Rechts der Cybersecurity unterstützen und insoweit auch über die notwendige Kompetenz zur Rechtsverbindlichkeit – und damit Rechtssicherheit – verfügen.

Dass für eine derartige Rechtsverbindlichkeit und Rechtssicherheit dringender Bedarf besteht, wird mit einem Blick auf die künftige politische und wirtschaftliche Schlüsseltechnologie Künstliche Intelligenz besonders deutlich, denn auch wenn die Volksrepublik China im kommenden Jahrzehnt die weltweite Technologieführerschaft für diesen Bereich für sich beansprucht, so befinden sich dennoch viele der in diesem Beitrag vorgestellten und diskutierten Regulierungsansätze in den unterschiedlichen

Cybersecurity-Gesetzen noch im Anfangsstadium. Für die KI-Regulierung im Zusammenhang mit der IT-Sicherheit ist ferner auffällig, dass es sich um einen klassischen Fall handelt, in dem das Recht den Risiken folgt, die sich aus der technologischen Entwicklung heraus ergeben – und es nicht umgekehrt das Recht ist, das zunächst die Rahmenbedingungen für sichere Technologieentwicklung und Einsatzszenarien setzt.

Die IT-Sicherheit von KI ist stets aus zwei unterschiedlichen Perspektiven zu betrachten: Einerseits sind die möglichen Einsatzszenarien zu berücksichtigen, die sich zur Verbesserung und Förderung der IT-Sicherheit durch KI-Maßnahmen ergeben können, andererseits sind die Risiken zu ermitteln und einzuschätzen, die eine fehlerhaft entwickelte KI für die IT-Sicherheit mit sich bringen kann. Dieser Dualismus findet sich in der gegenwärtigen Rechtslage noch kaum wieder – geht es doch in vielen IT-sicherheitsbezogenen Rechtsvorschriften der Volksrepublik nur darum, dass diese bewusst entwicklungsoffen und damit gleichermaßen unbestimmt formuliert sind, um die Möglichkeit zu bieten, KI als technisch-organisatorische Vorkehrung in die weiteren Rahmenbedingungen des chinesischen IT-Rechts aufzunehmen. Mit erheblicher Wahrscheinlichkeit wird man jedoch davon ausgehen können, dass die chinesische Gesetzgebung hier in den kommenden Jahren nach und nach weitere und auch konkretere Vorgaben zur sicheren KI-Nutzung entwickelt – nicht zuletzt auch deshalb, weil China die Entwicklung von KI-Technologien zu einer Hauptfrage der gegenwärtigen und zukünftigen technologischen Stoßrichtung des Landes gemacht hat. Nichtsdestotrotz dürfte gerade China mit Blick auf die KI-Gesetzgebung keine globale „model role" einnehmen, da chinesische Gesetze ihrer Natur nach bereits unbestimmt formuliert sind, unabhängig davon, ob es um KI, Cybersecurity oder um andere Themen geht – sie haben vielmehr den Charakter einer rechtspolitischen „Blaupause" für weitere und konkretere Maßnahmen in naher Zukunft. Umso mehr ergibt sich hier im internationalen Kontext auch die Chance für den EU-Gesetzgeber, transparente, verlässliche und einheitliche gesetzgeberische Vorgaben zu KI und Cybersecurity für den europäischen Binnenmarkt zu schaffen, um Unternehmen, Behörden und Verbraucher bei der (IT-) sicheren Entwicklung und Verwendung dieser neuen Technologie bestmöglich zu unterstützen. Schon für die EU DS-GVO hat sich nämlich in der Vergangenheit gezeigt, dass auch China den Blick auf Europa richtet.