Cybersicherheitsgesetz der Volksrepublik China (2016)

Deutsche Übersetzung des Cybersicherheitsgesetzes der Volksrepublik China (中华人民共和国网络安全法), erstellt von weber.cloud China

weber.cloud China ist eine Marke der
weber.digital GmbH
Bahnhofstraße 16, 72336 Balingen

Telefon +49 7433 21021-0
Web www.webercloud-china.de
E-Mail info@weber.cloud

Geschäftsführer
Dipl.-Inform.(FH) Jürgen Weber

Sitz der Gesellschaft Balingen
Handelsregister Amtsgericht Stuttgart
Registernr. HRB 411104
USt-IdNr. DE812928233

Bankverbindungen
Sparkasse Zollernalb
Kto. 24 055 969, BLZ 653 512 60
IBAN DE53 6535 1260 0024 0559 69
SWIFT/BIC-Code SOLA DE S1 BAL

Landesbank Baden-Württemberg
Kto. 24 601 29, BLZ 600 501 01
IBAN DE40 6005 0101 0002 4601 29
SWIFT/BIC-Code SOLA DE ST

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel I. Allgemeine Bestimmungen

Artikel 1
Dieses Gesetz dient der Gewährleistung der Cybersicherheit, dem Schutz der Souveränität des Cyberspace, der nationalen Sicherheit und des öffentlichen Interesses, dem Schutz der legitimen Rechte und Interessen von Bürgern, juristischen Personen und anderen Organisationen sowie der Förderung der gesunden Entwicklung der wirtschaftlichen und sozialen Informatisierung.

Artikel 2
Dieses Gesetz gilt für den Aufbau, den Betrieb, die Wartung und die Nutzung des Netzes sowie für die Überwachung und Verwaltung der Cybersicherheit auf dem Gebiet der Volksrepublik China.

Artikel 3
Der Staat besteht auf der Cybersicherheit und der informationsbasierten Entwicklung, befolgt die Richtlinien der positiven Nutzung, der wissenschaftlichen Entwicklung, der rechtlichen Verwaltung und der Sicherheitsgarantie, fördert den Aufbau der Netzinfrastruktur und der Vernetzung, unterstützt die Innovation und Anwendung von Netztechnologien, fördert die Ausbildung von Cybersicherheitspersonal, errichtet und verbessert das System zur Gewährleistung der Cybersicherheit und verbessert die Fähigkeit zum Schutz der Cybersicherheit.

Artikel 4
Der Staat arbeitet und verbessert laufend Cybersicherheitsstrategien aus, legt die grundlegenden Anforderungen und Hauptziele für die Gewährleistung der Cybersicherheit fest und schlägt Cybersicherheitsstrategien, Arbeitsaufgaben und Maßnahmen in Schlüsselbereichen vor.

Artikel 5
Der Staat ergreift Maßnahmen zur Überwachung, Abwehr und Bewältigung von Cybersicherheitsrisiken und -bedrohungen sowohl innerhalb als auch außerhalb des Hoheitsgebiets der Volksrepublik China, zum Schutz kritischer Informationsinfrastrukturen vor Angriffen, Eingriffen, Störungen und Schäden, zur Bestrafung illegaler Cyberkriminalität im Einklang mit dem Gesetz und zur Aufrechterhaltung der Sicherheit und Ordnung im Cyberspace.

Artikel 6
Der Staat setzt sich für ein ehrliches, vertrauenswürdiges, gesundes und zivilisiertes Verhalten im Netz ein, fördert die Verbreitung sozialistischer Grundwerte und ergreift Maßnahmen zur Stärkung des Bewusstseins und des Niveaus der Cybersicherheit in der gesamten Gesellschaft, um so ein günstiges Umfeld für die Förderung der Cybersicherheit unter Beteiligung der gesamten Gesellschaft zu schaffen.

Artikel 7
Der Staat führt aktiv den internationalen Austausch und die internationale Zusammenarbeit in Bezug auf die Verwaltung des Cyberspace, die Erforschung und Entwicklung von Netzwerktechnologien, die Formulierung entsprechender Standards und die Bekämpfung von

Cybersicherheitsgesetz der Volksrepublik China (2016)

Cyberkriminalität durch, fördert den Aufbau eines friedlichen, sicheren, offenen und kooperativen Cyberspace und errichtet ein multilaterales, demokratisches und transparentes System für die Verwaltung des Cyberspace.

Artikel 8
Die nationale Cyberspace-Verwaltung ist für die Gesamtplanung und Koordinierung der Cybersicherheitsarbeit und die entsprechende Überwachung und Verwaltung verantwortlich. Die zuständige Abteilung für Telekommunikation des Staatsrats, die Abteilungen für öffentliche Sicherheit und andere zuständige Behörden sind im Rahmen ihrer jeweiligen Funktionen gemäß den Bestimmungen dieses Gesetzes und anderer einschlägiger Gesetze und Verwaltungsvorschriften für den Schutz, die Überwachung und die Verwaltung der Cybersicherheit verantwortlich.

Die Aufgaben der zuständigen Abteilungen der lokalen Volksregierungen auf oder oberhalb der Kreisebene in Bezug auf den Schutz, die Überwachung und die Verwaltung der Cybersicherheit werden im Einklang mit den einschlägigen staatlichen Vorschriften festgelegt.

Artikel 9
Netzbetreiber müssen bei der Ausübung ihrer Geschäftstätigkeit und der Erbringung von Dienstleistungen die Gesetze und Verwaltungsvorschriften einhalten, die gesellschaftliche Moral respektieren, die Geschäftsethik beachten, ehrlich und vertrauenswürdig sein, der Verpflichtung zum Schutz der Cybersicherheit nachkommen, die Überwachung durch die Regierung und die Öffentlichkeit akzeptieren und soziale Verantwortung übernehmen.

Artikel 10
Für den Aufbau und den Betrieb des Netzes oder die Erbringung von Dienstleistungen über das Netz sind technische Maßnahmen und andere notwendige Maßnahmen gemäß den Bestimmungen der Rechts- und Verwaltungsvorschriften und den verbindlichen Anforderungen der nationalen Normen zu ergreifen, um die Netzsicherheit, einen stabilen Betrieb und eine wirksame Reaktion auf Cybersicherheitsvorfälle zu gewährleisten, illegale kriminelle Handlungen im Netz zu verhindern und die Integrität, Vertraulichkeit und Verfügbarkeit der Netzdaten zu wahren.

Artikel 11
Die Organisationen der netzgebundenen Wirtschaft verstärken im Einklang mit ihren Satzungen die Selbstregulierung der Wirtschaft, formulieren Verhaltenskodizes für die Cybersicherheit, weisen ihre Mitglieder an, den Schutz der Cybersicherheit zu verstärken, das Niveau des Schutzes der Cybersicherheit anzuheben und die gesunde Entwicklung der Wirtschaft zu fördern.

Artikel 12
Der Staat schützt die Rechte von Bürgern, juristischen Personen und anderen Organisationen, das Netz in Übereinstimmung mit dem Gesetz zu nutzen, fördert die Popularität des Netzzugangs, verbessert das Niveau der Netzdienste, stellt der Öffentlichkeit sichere und bequeme Netzdienste zur Verfügung und garantiert den geordneten und freien Fluss von Netzinformationen in Übereinstimmung mit dem Gesetz.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Jede Person oder Organisation, die das Internet nutzt, muss die Verfassung und die Gesetze einhalten, die öffentliche Ordnung befolgen und die soziale Ethik respektieren, darf die Cybersicherheit nicht gefährden und darf das Internet nicht für Aktivitäten nutzen, die die nationale Sicherheit, die Integrität und die Interessen des Landes gefährden, zur Untergrabung der Staatsmacht oder zum Umsturz des sozialistischen Systems anstiften, zur Spaltung des Landes oder zur Untergrabung der nationalen Einheit aufruft, Terrorismus oder Extremismus befürwortet, ethnischen Hass oder Diskriminierung propagiert, gewalttätige oder pornografische Informationen verbreitet, falsche Informationen fabriziert oder verbreitet, um die wirtschaftliche und soziale Ordnung zu stören, oder den Ruf, die Privatsphäre, die Rechte an geistigem Eigentum oder andere rechtmäßige Rechte und Interessen anderer Personen verletzt.

Artikel 13
Der Staat unterstützt die Erforschung und Entwicklung von Online-Produkten und -Dienstleistungen, die der gesunden Entwicklung von Minderjährigen förderlich sind, bestraft rechtlich die Aktivitäten, die die körperliche und geistige Gesundheit von Minderjährigen durch die Nutzung des Internets schädigen. Der Staat sorgt für eine sichere und gesunde Netzumgebung für Minderjährige.

Artikel 14
Jede Person oder Organisation hat das Recht, Handlungen, die die Cybersicherheit gefährden, bei der Verwaltung des Cyberspace, der Telekommunikationsabteilung, der Behörde für öffentliche Sicherheit und anderen Abteilungen zu melden. Die Dienststelle, die die Meldung erhält, bearbeitet eine solche Meldung zeitnah im Einklang mit dem Gesetz oder leitet die Meldung zeitnah an die zuständige Dienststelle weiter, wenn sie nicht in ihre Zuständigkeit fällt.

Die zuständige Dienststelle behandelt die Informationen über den Informanten vertraulich und schützt die gesetzlichen Rechte und Interessen des Informanten.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel II. Unterstützung und Förderung der Cybersicherheit

Artikel 15
Der Staat entwickelt und verbessert das System der Cybersicherheitsstandards. Die Verwaltungsabteilung für Normung des Staatsrats und andere einschlägige Abteilungen des Staatsrats organisieren im Einklang mit ihren jeweiligen Zuständigkeiten die Formulierung und rechtzeitige Überarbeitung nationaler und industrieller Normen für die Verwaltung der Cybersicherheit und die Sicherheit von Netzwerkprodukten, -diensten und -operationen.

Der Staat unterstützt Unternehmen, Forschungseinrichtungen, Hochschulen und netzbezogene Industrieorganisationen bei der Entwicklung nationaler und industrieller Normen für Cybersicherheit.

Artikel 16
Der Staatsrat und die Volksregierungen der Provinzen, autonomen Regionen und Kommunen, die direkt der Zentralregierung unterstehen, nehmen eine Gesamtplanung vor, erhöhen die Investitionen, unterstützen Schlüsselindustrien und -projekte der Cybersicherheitstechnologie, fördern die Forschung, Entwicklung und Anwendung von Cybersicherheitstechnologien, verbreiten sichere und zuverlässige Netzwerkprodukte und -dienste, schützen die Rechte des geistigen Eigentums an Netzwerktechnologien und unterstützen Unternehmen, Forschungseinrichtungen und Hochschulen u.a. bei der Teilnahme an nationalen Innovationsprojekten für Cybersicherheitstechnologien.

Artikel 17
Der Staat fördert den Aufbau eines sozialisierten Dienstleistungssystems für Cybersicherheit und ermutigt einschlägige Unternehmen und Institutionen, Sicherheitsdienstleistungen wie Cybersicherheitszertifizierung, -prüfung und -risikobewertung durchzuführen.

Artikel 18
Der Staat unterstützt die Entwicklung von Technologien zum Schutz und zur Nutzung von Netzdaten, fördert die Verfügbarkeit von öffentlichen Datenressourcen und die technologische Innovation sowie die soziale und wirtschaftliche Entwicklung.
Der Staat unterstützt die Innovation von Methoden des Cybersicherheitsmanagements und die Anwendung neuer Netzwerktechnologien zur Verbesserung des Cybersicherheitsschutzes.

Artikel 19
Die Volksregierungen auf allen Ebenen und ihre zuständigen Abteilungen organisieren eine regelmäßige Öffentlichkeitsarbeit, werben für Cybersicherheit und weisen die zuständigen Stellen an, die Öffentlichkeitsarbeit und Aufklärung über Cybersicherheit effektiv durchzuführen.

Die Massenmedien bieten der Öffentlichkeit relevante Information und Aufklärung über Cybersicherheit an.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 20
Der Staat unterstützt Unternehmen, Hochschulen, Berufsschulen und andere Ausbildungseinrichtungen bei der Durchführung von Ausbildungsmaßnahmen im Bereich der Cybersicherheit, ergreift vielfältige Maßnahmen zur Ausbildung von Netzsicherheitspersonal und fördert den Austausch von Netzsicherheitspersonal.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel III. Sicherheit des Netzbetriebs

Abschnitt 1: Allgemeine Bestimmungen

Artikel 21

Der Staat führt ein System zum Schutz der Cybersicherheitsebene ein. Die Netzbetreiber müssen gemäß den Anforderungen des Systems zum Schutz der Cybersicherheit die folgenden Sicherheitsverpflichtungen erfüllen, um sicherzustellen, dass das Netz frei von Störungen, Schäden oder unbefugtem Zugriff ist, und um zu verhindern, dass Netzdaten verraten, gestohlen oder gefälscht werden:

(1) Ausarbeitung interner Regeln für das Sicherheitsmanagement und Betriebsverfahren, Bestimmung der für die Cybersicherheit zuständigen Personen und Umsetzung der Verantwortlichkeiten für den Schutz der Cybersicherheit.

(2) Ergreifung technischer Maßnahmen zur Verhinderung von Computerviren, Netzangriffen, Eindringen in das Netz und anderen Handlungen, die die Cybersicherheit gefährden.

(3) Ergreifung technischer Maßnahmen zur Überwachung und Aufzeichnung des Status des Netzbetriebs und von Vorfällen im Bereich der Cybersicherheit sowie Aufbewahrung der entsprechenden Weblogs für mindestens sechs Monate, wie vorgeschrieben.

(4) Ergreifen von Maßnahmen wie Datenkategorisierung, Datensicherung und Verschlüsselung wichtiger Daten.

(5) Erfüllung sonstiger Verpflichtungen, die durch Gesetze und Verwaltungsvorschriften vorgeschrieben sind.

Artikel 22

Netzprodukte und -dienste müssen den verbindlichen Anforderungen der einschlägigen nationalen Normen entsprechen. Die Anbieter von Netzprodukten und -diensten dürfen keine Schadsoftware installieren. Stellt ein Anbieter ein Risiko wie einen Sicherheitsmangel oder eine Schwachstelle bei seinen Netzprodukten oder -diensten fest, so ergreift er unverzüglich Abhilfemaßnahmen, informiert die Nutzer rechtzeitig und meldet dies bei der zuständigen Stelle gemäß den einschlägigen Bestimmungen.

Die Anbieter von Netzprodukten und -diensten müssen kontinuierlich Sicherheitswartung für ihre Produkte und Dienste anbieten und dürfen die Bereitstellung der Sicherheitswartung nicht innerhalb der zwischen den Parteien festgelegten oder vereinbarten Frist kündigen.

Wenn Netzprodukte und -dienste die Funktion haben, Informationen über die Nutzer zu sammeln, müssen die Anbieter ihre Nutzer ausdrücklich darauf hinweisen und deren Zustimmung einholen. Sind personenbezogene Daten des Nutzers betroffen, so hat der Anbieter auch dieses Gesetz und die einschlägigen Rechts- und Verwaltungsvorschriften über den Schutz personenbezogener Daten einzuhalten.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 23
Wichtige Netzwerkausrüstungen und spezialisierte Cybersicherheitsprodukte müssen gemäß den verbindlichen Anforderungen der einschlägigen nationalen Normen die von qualifizierten Institutionen durchgeführte Sicherheitszertifizierung bestehen oder die Anforderungen der Sicherheitserkennung erfüllen, bevor sie verkauft oder bereitgestellt werden. Die nationale Cyberspace-Verwaltung entwickelt und veröffentlicht in Zusammenarbeit mit den zuständigen Abteilungen des Staatsrats den Katalog der wichtigsten Netzwerkausrüstungen und spezialisierten Cybersicherheitsprodukte und fördert die gegenseitige Anerkennung der Ergebnisse von Sicherheitszertifizierungen und Sicherheitstests, um wiederholte Zertifizierungen und Tests zu vermeiden.

Artikel 24
Erbringen Netzbetreiber Netzzugangs- und Domänenregistrierungsdienste für Nutzer, erledigen sie Netzzugangsformalitäten für Festnetz- oder Mobiltelefonnutzer oder stellen sie Nutzern Informationsfreigabedienste, Instant-Messaging-Dienste und andere Dienste zur Verfügung, so verlangen sie von den Nutzern die Angabe ihrer tatsächlichen Identität, wenn sie Verträge unterzeichnen oder die Bereitstellung von Diensten bestätigen. Wenn ein Nutzer seine echten Identitätsdaten nicht angibt, darf der Netzbetreiber ihm die entsprechenden Dienste nicht zur Verfügung stellen.

Der Staat setzt die Strategie der vertrauenswürdigen Identität im Cyberspace um, unterstützt die Erforschung und Entwicklung sicherer und bequemer Technologien für die elektronische Identitätsauthentifizierung und fördert die gegenseitige Anerkennung der verschiedenen Technologien zur elektronischen Identitätsauthentifizierung.

Artikel 25
Netzbetreiber müssen Notfallpläne für Vorfälle im Bereich der Cybersicherheit erstellen und sich rechtzeitig mit Systemfehlern, Computerviren, Netzangriffen, Netzeinbrüchen und anderen Sicherheitsrisiken befassen. Tritt ein Vorfall ein, der die Cybersicherheit gefährdet, so leitet der betreffende Betreiber unverzüglich den Notfallplan ein, ergreift die entsprechenden Abhilfemaßnahmen und meldet den Vorfall gemäß den einschlägigen Bestimmungen bei der zuständigen Stelle.

Artikel 26
Bei der Durchführung von Tätigkeiten wie der Zertifizierung der Netzsicherheit, der Durchführung von Tests, der Risikobewertung oder der Freigabe von Informationen über Systemschwachstellen, Computerviren, Netzangriffe, Eindringen in das Netz und andere Informationen zur Netzsicherheit an die Allgemeinheit sollten die einschlägigen nationalen Vorschriften eingehalten werden.

Artikel 27
Einzelpersonen und Organisationen dürfen sich nicht am illegalen Eindringen in fremde Netze, an der Störung der normalen Funktionen anderer Netze, am Diebstahl von Netzdaten und an anderen Aktivitäten beteiligen, die die Netzsicherheit gefährden; sie dürfen keine Programme und Werkzeuge bereitstellen, die speziell für das Eindringen in Netze, für die Störung der normalen

Cybersicherheitsgesetz der Volksrepublik China (2016)

Funktionen des Netzes und für Schutzmaßnahmen, für den Diebstahl von Netzdaten und für andere Aktivitäten bestimmt sind, die die Netzsicherheit gefährden; wenn sie wissen, dass andere an Aktivitäten beteiligt sind, die die Netzsicherheit gefährden, dürfen sie keine technische Unterstützung, Werbung und Verkaufsförderung, Zahlungsabwicklung und sonstige Hilfe leisten.

Artikel 28
Die Netzbetreiber sollten den Organen der öffentlichen Sicherheit und den Organen der nationalen Sicherheit, die zur Aufrechterhaltung der nationalen Sicherheit und zur Untersuchung von Straftaten gemäß den Gesetzen tätig sind, technische Unterstützung und Hilfe leisten.

Artikel 29
Der Staat unterstützt die Zusammenarbeit zwischen Netzbetreibern in Bereichen wie dem Sammeln, Analysieren, Melden und Reagieren auf Cybersicherheitsinformationen, um die Sicherheitsschutzkapazität der Netzbetreiber zu erhöhen.

Einschlägige Branchenverbände legen Regeln für den Schutz der Cybersicherheit und Koordinierungsmechanismen für ihre Branche fest, verstärken ihre Analyse und Bewertung der Cybersicherheit, führen innerhalb eines bestimmten Zeitraums Risikowarnungen für Mitglieder durch und unterstützen und koordinieren die Reaktionen der Mitglieder auf Cybersicherheitsrisiken.

Artikel 30
Informationen, die die Abteilung für Cybersicherheit und Informatisierung und die zuständigen Abteilungen bei der Durchführung von Aufgaben zum Schutz der Cybersicherheit erhalten, dürfen nur für Cybersicherheitszwecke und nicht für andere Zwecke verwendet werden.

Abschnitt 2: Betriebssicherheit für kritische Informationsinfrastrukturen

Artikel 31
Der Staat führt einen gezielten Schutz für kritische Informationsinfrastrukturen in wichtigen Sektoren und Bereichen wie öffentlichen Telekommunikations- und Informationsdiensten, Energie, Verkehr, Wasserressourcen, Finanzen, öffentlichen Diensten, elektronischen Behördendiensten usw. sowie für andere kritische Informationsinfrastrukturen ein, die im Falle ihrer Zerstörung, des Verlusts ihrer Funktionsfähigkeit oder von Datenlecks die nationale Sicherheit, die nationale Wirtschaft, den Lebensunterhalt der Bevölkerung und das öffentliche Interesse ernsthaft gefährden können, und zwar auf der Grundlage des Schutzsystems auf Cybersicherheitsniveau. Die konkreten Bereiche der kritischen Informationsinfrastrukturen und die Regeln für den Schutz der Sicherheit werden vom Staatsrat formuliert.

Der Staat ermutigt Netzbetreiber, die nicht zu dem Aufbau der wichtigen Netzeinrichtungen und Informationssystemen gehören, sich freiwillig an dem System zum Schutz kritischer Informationsinfrastrukturen zu beteiligen.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 32
Die für den Schutz kritischer Informationsinfrastrukturen zuständigen Abteilungen formulieren und organisieren im Rahmen der vom Staatsrat übertragenen Zuständigkeiten die Umsetzung von Sicherheitsplänen für kritische Informationsinfrastrukturen in der jeweiligen Branche oder im jeweiligen Bereich, leiten und überwachen die Arbeit an dem Schutz kritischer Informationsinfrastrukturen.

Artikel 33
Kritische Informationsinfrastrukturen sollten so aufgebaut werden, dass sie über die nötige Leistung verfügen, um den stabilen und kontinuierlichen Betrieb des Unternehmens zu unterstützen. Sie gewährleistet auch, dass Sicherheits- und technische Maßnahmen gleichzeitig geplant, gebaut und genutzt werden.

Artikel 34
Zusätzlich zu den Bestimmungen des Artikels 21 dieses Gesetzes haben die Betreiber kritischer Informationsinfrastrukturen die folgenden Sicherheitsaufgaben zu erfüllen:
(1) Sie richten spezialisierte Einrichtungen für das Sicherheitsmanagement und für das Sicherheitsmanagement verantwortliche Personen ein und müssen die verantwortliche Personen und die Personal in Schüsselpositionen wegen der Sicherheit überprüfen;
(2) Sie führen regelmäßig Schulungen zur Cybersicherheit, technische Schulungen und Kompetenzbewertungen für ihre Mitarbeiter durch;
(3) Durchführung von Notfall-Backups wichtiger Systeme und Datenbanken;
(4) Ausarbeitung von Notfallplänen für Cybersicherheitsvorfälle und regelmäßige Durchführung von Übungen;
(5) Sonstige Verpflichtungen gemäß den gesetzlichen Bestimmungen oder Verwaltungsvorschriften.

Artikel 35
Betreiber kritischer Informationsinfrastrukturen, die Netzwerkprodukte und -dienste erwerben, die die nationale Sicherheit beeinflussen könnten, müssen sich einer Sicherheitsinspektion unterziehen, die von der nationalen Cyberspace-Verwaltung und den zuständigen Abteilungen des Staatsrats organisiert wird.

Artikel 36
Betreiber kritischer Informationsinfrastrukturen, die Netzprodukte und -dienste erwerben, unterzeichnen mit den Anbietern eine Geheimhaltungsvereinbarung gemäß den Vorschriften, in der die Pflichten und Verantwortlichkeiten in Bezug auf Sicherheit und Vertraulichkeit festgelegt sind.

Artikel 37
Personenbezogene Informationen und wichtige Geschäftsdaten, die von Betreibern kritischer Informationsinfrastrukturen während ihrer Tätigkeit im Hoheitsgebiet der Volksrepublik China gesammelt und erstellt werden, sind im Hoheitsgebiet zu speichern; ist es aufgrund geschäftlicher Erfordernisse wirklich notwendig, sie außerhalb des chinesischen Festlands bereitzustellen, so ist eine Sicherheitsbewertung gemäß den von der nationalen Cyberspace-Verwaltung und den

Cybersicherheitsgesetz der Volksrepublik China (2016)

zuständigen Abteilungen des Staatsrats gemeinsam formulierten Maßnahmen durchzuführen. Wo Gesetze oder Verwaltungsvorschriften etwas anderes vorsehen, gelten diese Bestimmungen.

Artikel 38
Die Betreiber kritischer Informationsinfrastrukturen führen mindestens einmal jährlich entweder selbst oder durch Beauftragung einer spezialisierten Organisation eine Inspektion und Bewertung der Sicherheit ihrer Netze und der möglicherweise bestehenden Risiken durch und berichten der für den Sicherheitsschutz kritischer Informationsinfrastrukturen zuständigen Abteilung über den Stand der Überwachung und Bewertung sowie über Verbesserungsmaßnahmen.

Artikel 39
Die staatliche Abteilung für Cybersicherheit und Informatisierung koordiniert die zuständigen Abteilungen umfassend, um die folgenden Maßnahmen zum Schutz der Sicherheit kritischer Informationsinfrastrukturen zu ergreifen:
(1) Durchführung von Stichproben zu den Sicherheitsrisiken kritischer Informationsinfrastrukturen, Vorschlag von Verbesserungsmaßnahmen und, falls erforderlich, Ernennung von auf Cybersicherheit spezialisierten Inspektions- und Erkennungsinstitutionen, die die Prüfung und Bewertung von Sicherheitsrisiken vornehmen;
(2) Regelmäßige Organisation von Notfallübungen für Betreiber kritischer Informationsinfrastrukturen, um das Reaktionsniveau und die Koordinierung der Reaktionen auf Cybersicherheitsvorfälle zu verbessern;
(3) Förderung des Austauschs von Cybersicherheitsinformationen zwischen den zuständigen Abteilungen, den Betreibern kritischer Informationsinfrastrukturen, Einrichtungen für Cybersicherheitsdienste und einschlägigen Forschungseinrichtungen;
(4) Bereitstellung von technischer Unterstützung und Hilfe für das Notfallmanagement und die Wiederherstellung der Cybersicherheit usw.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel IV. Sicherheit von Netzinformationen

Artikel 40
Die Netzbetreiber wahren die Vertraulichkeit der von ihnen erfassten Nutzerinformationen streng und richten Systeme zum Schutz der Nutzerinformationen ein und vervollständigen sie.

Artikel 41
Netzbetreiber, die personenbezogene Daten erheben und nutzen, müssen die Grundsätze der Rechtmäßigkeit, Zulässigkeit und Notwendigkeit beachten, ihre Regeln für die Erhebung und Nutzung von Daten veröffentlichen und dabei ausdrücklich den Zweck, die Mittel und den Umfang der Erhebung oder Nutzung von Daten angeben sowie die Zustimmung der Person einholen, deren Daten erhoben werden.

Die Netzbetreiber dürfen keine personenbezogenen Daten sammeln, die nicht im Zusammenhang mit den von ihnen angebotenen Diensten stehen; sie dürfen nicht gegen die Bestimmungen von Gesetzen, Verwaltungsvorschriften oder Vereinbarungen zwischen den Parteien verstoßen, um personenbezogene Daten zu sammeln oder zu verwenden; und sie müssen die Bestimmungen von Gesetzen, Verwaltungsvorschriften oder Vereinbarungen mit den Nutzern befolgen, um die von ihnen gespeicherten personenbezogenen Daten zu verarbeiten.

Artikel 42
Die Netzbetreiber dürfen die von ihnen gesammelten personenbezogenen Daten nicht weitergeben, verfälschen oder beschädigen; ohne die Zustimmung der Person, deren Daten gesammelt werden, dürfen personenbezogene Daten nicht an andere weitergegeben werden. Es sei denn, sie wurden in einer Weise verarbeitet, die es unmöglich macht, eine bestimmte Person zu identifizieren, und sie nicht zurückverfolgt werden können.

Die Netzbetreiber treffen die technischen und sonstigen erforderlichen Maßnahmen, um die Sicherheit der von ihnen gesammelten personenbezogenen Daten zu gewährleisten und ein Durchsickern von Informationen sowie deren Beschädigung oder Verlust zu verhindern. Tritt eine Situation ein, in der Informationen durchsickern, beschädigt werden oder verloren gehen könnten, ergreifen sie unverzüglich Abhilfemaßnahmen, benachrichtigen die Nutzer rechtzeitig und melden die Angelegenheit den zuständigen Stellen gemäß den Vorschriften.

Artikel 43
Stellt eine Person fest, dass Netzbetreiber bei der Erhebung oder Nutzung ihrer personenbezogenen Daten gegen Rechts- und Verwaltungsvorschriften oder Vereinbarungen zwischen den Parteien verstoßen haben, hat sie das Recht, von den Netzbetreibern die Löschung ihrer personenbezogenen Daten zu verlangen; stellt sie fest, dass die von den Netzbetreibern erhobenen oder gespeicherten personenbezogenen Daten Fehler enthalten, hat sie das Recht, von den Netzbetreibern Korrekturen zu verlangen. Die Netzbetreiber ergreifen Maßnahmen zur Löschung oder Berichtigung.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 44
Einzelpersonen oder Organisationen dürfen personenbezogene Daten nicht stehlen oder andere illegale Methoden anwenden, um an sie zu gelangen, und sie dürfen personenbezogene Daten der Bürger nicht verkaufen oder anderen unrechtmäßig zur Verfügung stellen.

Artikel 45
Dienststellen und ihr Personal, die gemäß dem Gesetz mit der Überwachung und Verwaltung der Cybersicherheit betraut sind, müssen persönliche Informationen, private Informationen und Geschäftsgeheimnisse, von denen sie bei der Erfüllung ihrer Aufgaben Kenntnis erlangen, streng vertraulich behandeln und dürfen sie nicht weitergeben, verkaufen oder anderen unrechtmäßig zur Verfügung stellen.

Artikel 46
Jede Person und Organisation sind bei der Nutzung des Internets für ihre Handlungen verantwortlich. Sie dürfen nicht zulassen, dass Websites oder Kommunikationsgruppen eingerichtet werden, die dazu dienen, Betrug zu begehen, kriminelle Methoden zu verbreiten, verbotene oder kontrollierte Güter herzustellen oder zu verkaufen oder sonstige rechtswidrige und kriminelle Handlungen zu begehen; sie dürfen das Netz nicht zur Verbreitung von Informationen über die Begehung von Betrug, die Herstellung oder den Verkauf verbotener und kontrollierter Güter oder sonstige rechtswidrige und kriminelle Handlungen nutzen.

Artikel 47
Die Netzbetreiber haben die Verwaltung der von den Nutzern veröffentlichten Informationen zu verstärken, und wenn sie Informationen entdecken, deren Veröffentlichung oder Verbreitung nach den Gesetzen und Vorschriften verboten ist, haben sie die Verbreitung dieser Informationen unverzüglich zu stoppen, Maßnahmen wie z. B. die Informationen zu löschen, die Verbreitung der Informationen zu verhindern, einschlägige Aufzeichnungen zu speichern und die zuständigen Stellen zu unterrichten.

Artikel 48
Die von Einzelpersonen und Organisationen übermittelten elektronischen Informationen und die von ihnen bereitgestellte Anwendungssoftware dürfen nicht mit bösartigen Programmen versehen sein und keine Informationen enthalten, deren Veröffentlichung oder Übermittlung durch Gesetze oder Verwaltungsvorschriften verboten ist.
Anbieter von Diensten für die Verbreitung elektronischer Informationen und Anbieter von Diensten für das Herunterladen von Anwendungssoftware müssen Sicherheitsverwaltungsaufgaben wahrnehmen; wenn sie wissen, dass ihre Benutzer Handlungen im Sinne des vorstehenden Absatzes begehen, müssen sie die Bereitstellung von Diensten einstellen und Maßnahmen wie das Löschen von Daten ergreifen, die entsprechenden Aufzeichnungen speichern und den zuständigen Abteilungen Bericht erstatten.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 49
Die Netzbetreiber richten Beschwerde- und Meldesysteme für die Netzinformationssicherheit ein, veröffentlichen Informationen wie die Methoden für die Einreichung von Beschwerden oder Meldungen und nehmen Beschwerden und Meldungen, die die Netzinformationssicherheit betreffen, unverzüglich entgegen und bearbeiten sie.
Die Netzbetreiber arbeiten mit den Abteilungen für Cybersicherheit und Informatisierung und den zuständigen Abteilungen zusammen, wenn die Abteilungen gemäß dem Gesetz sie überwachen oder untersuchen müssen.

Artikel 50
Die staatlichen Internet-Informationsabteilungen und die zuständigen Abteilungen nehmen ihre Pflichten zur Überwachung und Verwaltung der Sicherheit von Netzinformationen in Übereinstimmung mit dem Gesetz wahr. Wenn sie Informationen entdecken, deren Veröffentlichung oder Weitergabe durch Gesetze oder Verwaltungsvorschriften verboten ist, fordern sie den Netzbetreiber auf, die Weitergabe zu stoppen, Entsorgungsmaßnahmen wie die Beseitigung zu ergreifen und entsprechende Aufzeichnungen zu führen. Bei den oben beschriebenen Informationen, die von außerhalb der Volksrepublik China stammen, benachrichtigen sie die zuständigen Institutionen, um technische Maßnahmen und andere notwendige Maßnahmen zu ergreifen, um die Übermittlung von Informationen zu blockieren.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel V. Überwachung, Frühwarnung und Notfallmaßnahmen

Artikel 51
Der Staat richtet Systeme zur Überwachung der Cybersicherheit, zur Frühwarnung und zur Meldung von Informationen ein. Die nationale Cyberspace-Verwaltung übernimmt die Gesamtkoordinierung der zuständigen Abteilungen, um die Sammlung, Analyse und Berichterstattung von Cybersicherheitsinformationen zu verstärken, und veröffentlicht einheitliche Cybersicherheitsüberwachungs- und Frühwarninformationen in Übereinstimmung mit den Vorschriften.

Artikel 52
Abteilungen, die für den Schutz kritischer Informationsinfrastrukturen zuständig sind, richten Systeme zur Überwachung und Frühwarnung im Bereich der Cybersicherheit und zur Meldung von Informationen für ihre jeweilige Branche oder ihren jeweiligen Bereich ein und verbessern diese und melden Informationen zur Überwachung und Frühwarnung im Bereich der Cybersicherheit gemäß den Vorschriften.

Artikel 53
Die nationale Cyberspace-Administration koordiniert sich mit den zuständigen Abteilungen, um einen Mechanismus für die Bewertung der Netzsicherheitsrisiken und die Reaktion auf Notfälle einzurichten, und Notfallpläne für Cybervorfälle zu entwickeln. Außerdem muss die nationale Cyberspace-Administration regelmäßig eine Übung durchführen.

Der Notfallplan für Sicherheitsvorfälle im Netz sollte Sicherheitsvorfälle im Netz nach dem Grad des Schadens nach dem Vorfall und dem Ausmaß der Auswirkungen und anderen Faktoren klassifizieren und entsprechende Notfallmaßnahmen vorsehen.

Artikel 54
Bei drohenden oder wahrscheinlichen Vorfällen im Bereich der Cybersicherheit ergreifen die zuständigen Abteilungen der Volksregierungen auf Provinz- und höherer Ebene im Einklang mit den vorgeschriebenen Zuständigkeiten und Verfahren sowie den Merkmalen des Cybersicherheitsrisikos und des möglichen Schadens die folgenden Maßnahmen:
(1) Sie verlangen, dass die zuständigen Abteilungen, Institutionen und das Personal umgehend relevante Informationen sammeln und melden und die Überwachung von Cybersicherheitsrisiken verstärken;
(2) Organisieren Sie relevante Abteilungen, Institutionen und Fachpersonal, um eine Analyse und Bewertung der Daten von Cybersicherheitsvorfällen vorzunehmen und die Wahrscheinlichkeit des Auftretens, den Umfang der Auswirkungen und das Ausmaß des Schadens vorherzusagen;
(3) Warnungen über die Cybersicherheitsrisiken für die Gesellschaft herausgeben und Maßnahmen zur Schadensvermeidung oder -minderung veröffentlichen.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 55
Beim Auftreten von Cybersicherheitsvorfällen wird unverzüglich ein Notfallplan für Cybersicherheitsvorfälle eingeleitet, eine Bewertung und Beurteilung des Cybersicherheitsvorfalls durchgeführt, die Netzbetreiber werden aufgefordert, technische und andere notwendige Maßnahmen zu ergreifen, potenzielle Sicherheitsrisiken zu beseitigen, die Ausbreitung von Schäden zu verhindern und unverzüglich Warnungen an die Öffentlichkeit zu richten.

Artikel 56
Stellen die zuständigen Abteilungen der Volksregierungen auf Provinz- oder höherer Ebene bei der Wahrnehmung ihrer Aufsichts- und Verwaltungsaufgaben im Bereich der Cybersicherheit fest, dass Netze ein großes Sicherheitsrisiko aufweisen, oder stellen sie Sicherheitsvorfälle fest, so können sie im Einklang mit den vorgeschriebenen Zuständigkeiten und Verfahren ein Gespräch mit dem gesetzlichen Vertreter oder den Hauptverantwortlichen des Betreibers dieses Netzes führen. Die Netzbetreiber ergreifen Maßnahmen zur Behebung der Situation und zur Beseitigung von Gefahren entsprechend den Anforderungen.

Artikel 57
Treten plötzliche Notfälle oder Produktionssicherheitsunfälle aufgrund von Vorfällen im Bereich der Cybersicherheit auf, so sind sie gemäß dem "Emergency Response Law of the People's Republic of China" und dem "Production Safety Law of the People's Republic of China" sowie anderen einschlägigen Gesetzen und Verwaltungsvorschriften zu behandeln.

Artikel 58
Um der Notwendigkeit des Schutzes der nationalen Sicherheit und der sozialen öffentlichen Ordnung gerecht zu werden und um auf schwerwiegende Vorfälle im Bereich der sozialen Sicherheit zu reagieren, können mit Genehmigung oder auf Beschluss des Staatsrats vorübergehende Maßnahmen in Bezug auf die Netzkommunikation in bestimmten Regionen ergriffen werden, wie z. B. die Einschränkung der Kommunikation.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel VI. Rechtliche Verantwortung

Artikel 59
Wenn Netzbetreiber ihren Verpflichtungen zum Schutz der Netzsicherheit gemäß den Artikeln 21 und 25 dieses Gesetzes nicht erfüllen, ordnen die zuständigen Abteilungen Korrekturen an und erteilen Verwarnungen; wenn Korrekturen verweigert werden oder dies zu einer Gefährdung der Cybersicherheit oder anderen derartigen Folgen führt, wird eine Geldstrafe zwischen 10.000 Yuan und 100.000 Yuan verhängt; das direkt verantwortliche Führungspersonal wird mit einer Geldstrafe zwischen 5.000 Yuan und 50.000 Yuan belegt.

Wenn Betreiber kritischer Informationsinfrastrukturen die in den Artikeln 33, 34, 36 und 38 dieses Gesetzes vorgesehenen Pflichten zum Schutz der Cybersicherheit nicht erfüllen, ordnen die zuständigen Abteilungen Korrekturen an und erteilen Verwarnungen; wenn Korrekturen verweigert werden oder dies zu einer Gefährdung der Cybersicherheit oder anderen derartigen Folgen führt, wird eine Geldstrafe zwischen 100.000 Yuan und 1.000.000 Yuan verhängt; gegen das direkt verantwortliche Führungspersonal wird eine Geldstrafe zwischen 10.000 Yuan und 100.000 Yuan verhängt.

Artikel 60
Bei Verstößen gegen Artikel 22 Absätze 1 und 2 oder Artikel 48 Absatz I ordnet die zuständige Abteilung Korrekturen an und spricht Verwarnungen aus; werden Korrekturen verweigert oder führt dies zu einer Gefährdung der Cybersicherheit oder anderen Folgen, wird eine Geldstrafe zwischen 50.000 Yuan und 500.000 Yuan verhängt; die direkt verantwortlichen Personen werden mit einer Geldstrafe zwischen 10.000 Yuan und 100.000 Yuan belegt:
(1) Installation von bösartigen Programmen;
(2) Wenn Risiken wie Sicherheitsmängel oder Schwachstellen in ihren Produkten oder Dienstleistungen bestehen, sie aber nicht sofort Abhilfemaßnahmen ergreifen oder die Nutzer nicht rechtzeitig informieren und die Angelegenheit den zuständigen Kontrollabteilungen gemäß den Vorschriften melden;
(3) Die unbefugte Beendigung der Sicherheitswartung ihrer Produkte und Dienstleistungen.

Artikel 61
Netzbetreiber, die gegen die Bestimmungen von Artikel 24 Absatz 1 dieses Gesetzes verstoßen, indem sie es unterlassen, von den Nutzern echte Identitätsangaben zu verlangen oder Nutzern, die keine echten Identitätsangaben machen, entsprechende Dienste anzubieten, werden von der jeweils zuständigen Abteilung zu Korrekturen aufgefordert; werden Korrekturen verweigert oder sind die Umstände schwerwiegend, wird eine Geldstrafe zwischen 50. 000 Yuan und 500.000 Yuan verhängt, und die jeweils zuständige Abteilung kann eine vorübergehende Aussetzung des Betriebs, eine Aussetzung des Geschäftsbetriebs für Korrekturen, die Schließung von Websites, den Widerruf der entsprechenden Betriebsgenehmigungen oder die Aufhebung von Geschäftslizenzen anordnen; direkt verantwortliche Personen und anderes direkt verantwortliches Personal werden mit Geldstrafen zwischen 10.000 Yuan und 100.000 Yuan belegt.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 62
Diejenigen, die unter Verstoß gegen die Bestimmungen von Artikel 26 dieses Gesetzes Cybersicherheitszertifizierungen, -tests oder -risikobewertungen durchführen oder Cybersicherheitsinformationen wie Systemlecks, Computerviren, Cyberangriffe usw. an die Gesellschaft veröffentlichen, werden von den zuständigen Abteilungen aufgefordert, die Angelegenheiten zu berichtigen und werden verwarnt; wenn die Berichtigung verweigert wird oder die Umstände schwerwiegend sind, wird eine Geldstrafe von 10. 000 Yuan bis 100.000 Yuan verhängt, und die zuständige Kontrollabteilung kann eine vorübergehende Aussetzung des Geschäftsbetriebs, eine Aussetzung des Geschäftsbetriebs zur Berichtigung, die Schließung von Websites, die Aufhebung der entsprechenden Geschäftsgenehmigungen oder den Entzug der Geschäftslizenz anordnen; direkt verantwortliche Personen und andere direkt Verantwortliche werden mit Geldstrafen von mindestens 5.000 Yuan und höchstens 50.000 Yuan belegt.

Artikel 63
Wer gegen die Bestimmungen von Artikel 27 dieses Gesetzes verstößt, indem er Tätigkeiten ausübt, die die Netzsicherheit gefährden, oder indem er Programme oder Hilfsmittel bereitstellt, die speziell für die Ausübung von Tätigkeiten konzipiert sind, die die Netzsicherheit gefährden, oder indem er technische Unterstützung, Werbung und Verkaufsförderung, Zahlungen und Abwicklungshilfe für andere leistet, damit diese Tätigkeiten ausüben, die die Netzsicherheit gefährden, die aber noch keinen Straftatbestand erfüllen, wird von den öffentlichen Sicherheitsbehörden beschlagnahmt, mit einer Haftstrafe von bis zu fünf Tagen belegt und kann zusätzlich mit einer Geldstrafe von mindestens 50.000 Yuan und höchstens 500.000 Yuan belegt werden; bei schwerwiegenden Fällen sind sie mit fünf bis fünfzehn Tagen Haft zu bestrafen, und zusätzlich kann eine Geldstrafe von 100.000 bis 1.000.000 Yuan verhängt werden.

Wenn eine Einheit Handlungen im Sinne des vorigen Absatzes begehen, beschlagnahmt das Organ für öffentliche Sicherheit die unrechtmäßigen Einkünfte, verhängt eine Geldstrafe von 100.000 bis 1.000.000 Yuan und bestraft die direkt verantwortliche Person und andere verantwortliche Personen gemäß den Bestimmungen des vorigen Absatzes.

Personen, die gegen die Bestimmungen von Artikel 27 dieses Gesetzes verstoßen und von der Verwaltung der öffentlichen Sicherheit bestraft werden, dürfen fünf Jahre lang nicht in Schlüsselpositionen des Cybersicherheitsmanagements und des Netzbetriebs arbeiten; Personen, die strafrechtlich bestraft werden, dürfen lebenslang nicht in Schlüsselpositionen des Cybersicherheitsmanagements und des Netzbetriebs arbeiten.

Artikel 64
Netzbetreiber und Anbieter von Netzprodukten oder -diensten, die gegen Artikel 22 Absatz 3 und die Artikel 41 bis 43 dieses Gesetzes verstoßen, indem sie den Schutz und die Rechte der persönlichen Daten der Bürger verletzen, werden von der jeweils zuständigen Stelle zu Korrekturen aufgefordert und können je nach den Umständen verwarnt, die unrechtmäßigen Gewinne eingezogen und/oder mit einer Geldstrafe in Höhe des 1- bis 10-fachen der unrechtmäßigen Gewinne belegt werden; liegen keine unrechtmäßigen Gewinne vor, wird eine Geldstrafe bis zu ein Million Yuan verhängt. Die unmittelbar verantwortliche Person und andere unmittelbar

Cybersicherheitsgesetz der Volksrepublik China (2016)

verantwortliche Personen werden mit Geldstrafe von mindestens 10.000 Yuan bis zu 100.000 Yuan verhängt. Wenn die Umstände schwerwiegend sind, kann die zuständige Abteilung eine vorübergehende Aussetzung der Geschäftstätigkeit, eine Aussetzung der Geschäftstätigkeit für Korrekturen, die Schließung von Websites, den Widerruf der entsprechenden Betriebsgenehmigungen oder die Aufhebung der Geschäftslizenzen anordnen.

Wird gegen Artikel 44 dieses Gesetzes verstoßen, indem personenbezogene Daten der Bürger gestohlen oder mit anderen illegalen Mitteln beschafft, illegal verkauft oder anderen illegal zur Verfügung gestellt werden, ohne dass dies eine Straftat darstellt, beschlagnahmen die Organe der öffentlichen Sicherheit die unrechtmäßig erzielten Gewinne und verhängen eine Geldstrafe in Höhe des ein- bis zehnfachen Betrags der unrechtmäßig erzielten Gewinne, und wenn keine unrechtmäßig erzielten Gewinne vorliegen, verhängen sie eine Geldstrafe von bis zu 1.000.000 Yuan.

Artikel 65
Verstoßen Betreiber kritischer Informationsinfrastrukturen gegen Artikel 35 dieses Gesetzes, indem sie Netzprodukte oder -dienste nutzen, die nicht sicherheitsüberprüft wurden oder die Sicherheitsüberprüfung nicht bestanden haben, ordnen die zuständigen Abteilungen an, die Nutzung zu beendigen, und verhängen eine Geldstrafe in Höhe des 1- bis 10-fachen des Kaufpreises; gegen die unmittelbar verantwortlichen Personen und andere unmittelbar verantwortliche Personen werden Geldstrafen zwischen 10.000 Yuan und 100.000 Yuan verhängt.

Artikel 66
Wenn Betreiber kritischer Informationsinfrastrukturen gegen die Bestimmungen von Artikel 37 dieses Gesetzes verstoßen, indem sie Netzdaten außerhalb des Festlandgebiets speichern oder Netzdaten an eine Einrichtung oder eine Person außerhalb des Festlandgebiets weitergeben, ordnet die jeweils zuständige Abteilung Korrekturen an, erteilt Verwarnungen, beschlagnahmt unrechtmäßige Gewinne, verhängt Geldbußen zwischen 50. 000 Yuan und 500.000 Yuan und kann eine vorübergehende Aussetzung des Betriebs, eine Aussetzung des Geschäftsbetriebs für Korrekturen, die Schließung von Websites, den Widerruf der entsprechenden Betriebsgenehmigungen oder die Annullierung von Geschäftslizenzen anordnen; direkt verantwortliche Personen und anderes direkt verantwortliches Personal werden mit Geldstrafen zwischen 10.000 Yuan und 100.000 Yuan belegt.

Artikel 67
Diejenigen, die unter Verstoß gegen Artikel 46 dieses Gesetzes Websites oder Kommunikationsgruppen zur Begehung illegaler oder krimineller Aktivitäten einrichten oder das Internet zur Veröffentlichung von Informationen im Zusammenhang mit der Begehung illegaler oder krimineller Aktivitäten nutzen, ohne dass eine Straftat begangen wurde, werden von den Organen der öffentlichen Sicherheit für höchstens fünf Tage inhaftiert und mit einer Geldstrafe von 10. 000 Yuan oder mehr, aber weniger als 100.000 Yuan verhängt werden; bei schwerwiegenden Umständen wird eine Haftstrafe von fünf Tagen oder mehr, aber weniger als fünfzehn Tagen verhängt, und eine Geldstrafe von 50.000 Yuan oder mehr, aber weniger als 500.000 Yuan kann

Cybersicherheitsgesetz der Volksrepublik China (2016)

zusätzlich verhängt werden. Die für illegale oder kriminelle Aktivitäten genutzten Websites und Kommunikationsgruppen werden ebenfalls geschlossen.

Die Organe der öffentlichen Sicherheit verhängen Geldstrafen in Höhe von 100.000 Yuan oder mehr, aber weniger als 500.000 Yuan, und die direkt verantwortliche Person und andere direkt verantwortliche Personen werden gemäß den Bestimmungen des vorangegangenen Absatzes bestraft, wenn sich Einheiten an den im vorstehenden Absatz genannten Handlungen beteiligt haben.

Artikel 68
Wenn Netzbetreiber gegen Artikel 47 dieses Gesetzes verstoßen, indem sie die Übermittlung von Informationen, deren Veröffentlichung oder Übermittlung durch Gesetze oder Verwaltungsvorschriften verboten ist, nicht unterbrechen, keine Maßnahmen zur Beseitigung ergreifen, wie z. B. die Löschung, oder die entsprechenden Aufzeichnungen nicht speichern, ordnet die jeweils zuständige Abteilung Korrekturen an, spricht Verwarnungen aus und beschlagnahmt unrechtmäßige Gewinne; wenn Korrekturen verweigert werden oder die Umstände schwerwiegend sind, können Geldstrafen zwischen 100.000 und 500.000 Yuan verhängt, und es kann eine vorübergehende Aussetzung des Betriebs, eine Aussetzung des Geschäftsbetriebs für Korrekturen, die Schließung von Websites, der Entzug der entsprechenden Betriebsgenehmigungen oder die Aufhebung von Geschäftslizenzen angeordnet werden; direkt verantwortliche Personen und anderes direkt verantwortliches Personal werden mit Geldstrafen zwischen 10.000 und 100.000 Yuan belegt.

Anbieter von elektronischen Informationsdiensten und Anbieter von Diensten zum Herunterladen von Anwendungssoftware, die ihren Pflichten zum Sicherheitsmanagement gemäß Artikel 48 Absatz 2 dieses Gesetzes nicht nachgekommen sind, werden gemäß den Bestimmungen des vorherigen Absatzes bestraft.

Artikel 69
Netzbetreiber, die gegen die Bestimmungen dieses Gesetzes verstoßen, indem sie eine der folgenden Handlungen begehen, werden von der jeweils zuständigen Abteilung aufgefordert, Korrekturen vorzunehmen; wenn sie sich weigern, Korrekturen vorzunehmen, oder die Umstände schwerwiegend sind, werden sie mit einer Geldstrafe von mindestens 50.000 Yuan bis zu 500.000 Yuan belegt; das verantwortliche Personal, das direkt haftbar ist, und anderes direkt haftbares Personal werden mit einer Geldstrafe von mindestens 10.000 Yuan bis zu 100.000 Yuan belegt:
(1) Unterlassung von Beseitigungsmaßnahmen wie die Unterbrechung der Übermittlung oder die Beseitigung von Informationen, deren Veröffentlichung oder Übermittlung durch Gesetze oder Verwaltungsvorschriften verboten ist, gemäß den Anforderungen der zuständigen Abteilungen;
(2) die rechtmäßige Überwachung und Kontrolle der zuständigen Abteilungen verweigern oder behindern;
(3) Weigerung, den Organen der öffentlichen Sicherheit und den Organen der nationalen Sicherheit die erforderliche technische Unterstützung und Hilfe zu leisten.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 70
Diejenigen, die Informationen veröffentlichen oder übermitteln, deren Veröffentlichung oder Übermittlung nach Artikel 12 Absatz 2 dieses Gesetzes oder nach anderen Gesetzen und Verwaltungsvorschriften verboten ist, werden gemäß den Bestimmungen der einschlägigen Gesetze und Verwaltungsvorschriften bestraft.

Artikel 71
Handlungen, die unter Verstoß gegen die Bestimmungen dieses Gesetzes begangen werden, werden gemäß den Bestimmungen der einschlägigen Rechts- und Verwaltungsvorschriften in Kreditakten eingetragen und veröffentlicht.

Artikel 72
Wenn ein Betreiber eines staatlichen Dienstleistungsnetzes einer staatlichen Organisation die in diesem Gesetz vorgeschriebenen Pflichten zum Schutz der Cybersicherheit nicht erfüllt, ordnet die übergeordnete Organisation oder die zuständigen Abteilungen Korrekturen an; die direkt verantwortlichen Manager und andere direkt verantwortliche Mitarbeiter werden bestraft.

Artikel 73
Wenn die Cyberspace Administration von China und die zuständigen Abteilungen gegen die Bestimmungen von Artikel 30 dieses Gesetzes verstoßen und Informationen, die sie bei der Erfüllung ihrer Aufgaben zum Schutz der Cybersicherheit erlangt haben, für andere Zwecke verwenden, werden die direkt verantwortliche Person und andere direkt verantwortliche Mitarbeiter gemäß dem Gesetz bestraft.

Vernachlässigt ein Personal der Cyberspace Administration von China und der zuständigen Abteilungen seine Pflichten, missbraucht es seine Macht oder verfälscht es das Gesetz zum persönlichen Vorteil, ohne dass dies eine Straftat darstellt, wird er gemäß dem Gesetz bestraft.

Artikel 74
Werden durch Verstöße gegen die Bestimmungen dieses Gesetzes andere Personen geschädigt, so wird die zivilrechtliche Haftung gemäß den gesetzlichen Bestimmungen übernommen.

Jede Person, die gegen die Bestimmungen dieses Gesetzes verstößt und einen Verstoß gegen die Verwaltung der öffentlichen Sicherheit begeht, wird gemäß dem Gesetz mit einer Strafe der Verwaltung der öffentlichen Sicherheit belegt; begeht sie ein Verbrechen, wird sie gemäß dem Gesetz mit strafrechtlicher Verantwortung verhängt.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Artikel 75

Wenn ausländische Institutionen, Organisationen oder Einzelpersonen Angriffe, Eingriffe, Störungen, Zerstörungen und andere Handlungen begehen, die die kritische Informationsinfrastruktur der Volksrepublik China schädigen und schwerwiegende Folgen nach sich ziehen, wird die strafrechtliche Verantwortung nach dem Gesetz verfolgt. Die für die öffentliche Sicherheit zuständigen Abteilungen des Staatsrats und die zuständigen Abteilungen können auch beschließen, die Vermögenswerte der genannten Einrichtungen, Organisationen oder Einzelpersonen einzufrieren oder andere notwendige Strafmaßnahmen zu ergreifen.

Cybersicherheitsgesetz der Volksrepublik China (2016)

Kapitel VII. Ergänzende Bestimmungen

Artikel 76
In diesem Gesetz haben die nachstehenden Begriffe die folgende Bedeutung:
(1) "Netze" bezieht sich auf ein System, das aus Computern oder anderen Informationsendgeräten und zugehöriger Ausrüstung besteht, die bestimmten Regeln und Verfahren für die Sammlung, Speicherung, Übertragung, den Austausch und die Verarbeitung von Informationen folgen.
(2) "Cybersicherheit" bezieht sich auf die Ergreifung der erforderlichen Maßnahmen zur Verhinderung von Angriffen, Eingriffen, Störungen, Sabotage und unrechtmäßiger Nutzung von Netzen sowie unerwarteten Unfällen, um einen stabilen und zuverlässigen Betrieb der Netze zu gewährleisten und die Integrität, Geheimhaltung und Nutzbarkeit von Netzinformationen zu sichern.
(3) "Netzbetreiber" bezieht sich auf die Eigentümer und Verwalter von Netzen sowie auf Anbieter von Netzdiensten.
(4) "Netzdaten" bezieht sich auf alle Arten von elektronischen Daten, die über Netze erfasst, gespeichert, übertragen, verarbeitet und erzeugt werden.
(5) "Personenbezogene Daten" sind alle in elektronischer oder sonstiger Form gespeicherten Informationen, die einzeln oder zusammen mit anderen Informationen die Feststellung der Identität einer natürlichen Person ermöglichen, einschließlich, aber nicht beschränkt auf Namen, Geburtsdatum, Personalausweisnummer, persönliche biometrische Daten, Anschrift, Telefonnummer usw.

Artikel 77
Der betriebliche Sicherheitsschutz von Netzen, in denen Informationen, die Staatsgeheimnisse betreffen, gespeichert und verarbeitet werden, muss neben der Einhaltung dieses Gesetzes auch die Bestimmungen der Gesetze und Verwaltungsvorschriften über die Vertraulichkeit einhalten.

Artikel 78
Der Schutz der militärischen Netze und der Informationssicherheit wird von der zentralen Militärkommission gesondert geregelt.

Artikel 79
Dieses Gesetz tritt am 1. Juni 2017 in Kraft.