Cybersicherheitsgesetz der Volksrepublik China (Revision 2025)

中华人民共和国网络安全法（2025修正）

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过　根据2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议《关于修改<中华人民共和国网络安全法>的决定》修正）

目录

Cybersicherheitsgesetz der Volksrepublik China (Revision 2025)[1]

(Verabschiedet auf der 24. Sitzung des Ständigen Ausschusses des 12. Nationalen Volkskongresses am 7.11.2016[2]; geändert aufgrund des „Beschlusses zur Revision des ‚Cybersicherheitsgesetzes der Volksrepublik China'" der 18. Sitzung des Ständigen Ausschusses des 14. Nationalen Volkskongresses am 28.10.2025[3])

Inhalt

1 Chinesischer Text abrufbar unter <lawinfochina.com> [北大法律英文网]/<pkulaw.cn> [北大法宝], Indexnummer [法宝引证码] CLI.1.5322204.

2 Chinesisch-deutsche Fassung des Gesetzes in der Fassung vom 7.11.2016 abgedruckt in: ZChinR 2018, S. 113 ff.

3 Chinesischer Text des Beschlusses abrufbar unter <lawinfochina.com> [北大法律英文网]/<pkulaw.cn> [北大法宝], Indexnummer [法宝引证码] CLI.1.5321885.

4 Wörtlich: „gesetzliche".

ZChinR 2025: S. 349–374
DOI: 10.71163/zchinr.2025.349-374

第一章　总则

第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条　在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条　网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。

第四条　国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第五条　国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施

第六条　国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

1. Kapitel: Allgemeine Grundsätze

§ 1 [Normzweck; = § 1 a. F.] Um die Netzwerksicherheit zu gewährleisten, die Souveränität über den Cyberspace und die Staatssicherheit sowie allgemeine gesellschaftliche Interessen zu wahren, die legalen Rechte und Interessen der Bürger, juristischen Personen und anderen Organisationen zu gewährleisten [und] die gesunde Entwicklung der wirtschaftlichen und sozialen Informatisierung zu fördern, wurde dieses Gesetz festgelegt.

§ 2 [Anwendungsbereich; = § 2 a. F.] Bei Aufbau, Betrieb, Schutz und Nutzung eines Netzwerks innerhalb des Gebiets der Volksrepublik China sowie der Verwaltung der Aufsicht über die Netzwerksicherheit wird dieses Gesetz angewendet.

§ 3 [Führung der KPCh; neu eingefügt] Bei der Arbeit an der Netzwerksicherheit wird an der Führung der Kommunistischen Partei Chinas festgehalten, das umfassende Konzept der nationalen Sicherheit umgesetzt, Entwicklung und Sicherheit koordiniert und der Aufbau eines starken Netzwerkstaates gefördert.

§ 4 [Staatliche Ziele; = § 3 a. F.] Der Staat misst der Netzwerksicherheit und der Entwicklung der Informatisierung gleiches Gewicht zu,[5] folgt der Leitlinie aktiver Nutzung, wissenschaftlicher Entwicklung, rechtmäßiger Verwaltung und gewährleisteter Sicherheit, treibt den Aufbau der Netzwerkinfrastruktur und der Interkonnektivität voran, fördert Innovation und Gebrauch von Netzwerktechnologie,[6] unterstützt die Ausbildung qualifizierten Personals im Bereich der Netzwerksicherheit, errichtet ein starkes System zur Gewährleistung der Netzwerksicherheit [und] erhöht [so] die Fähigkeit zum Schutz der Netzwerksicherheit.

§ 5 [Strategie der Netzwerksicherheit; = § 4 a. F.] Der Staat legt eine Strategie zur Netzwerksicherheit fest und verbessert diese stetig, benennt klar die grundlegenden Erfordernisse und hauptsächlichen Ziele der Netzwerksicherheit [und] gibt für Schwerpunktbereiche die Netzwerksicherheitspolitik, Aufgaben[7] und Maßnahmen vor.

§ 6 [Schutz der Informationsinfrastruktur; = § 5 a. F.] Der Staat ergreift Maßnahmen zur Überwachung, Abwehr und Handhabung von Risiken für und Bedrohungen der Netzwerksicherheit von innerhalb oder außerhalb des Gebiets der Volksrepublik China, schützt die wesentliche Informationsinfrastruktur durch Abwendung von Angriffen, Eindringen, Störungen und Zerstörungen, bestraft dem Recht gemäß rechtswidrige, kriminelle Netzwerkaktivitäten [und] wahrt die Sicherheit und die Ordnung des Cyberspace.

5 Wörtlich: „hält an der gleichmäßigen Gewichtung ... fest“.

6 „技术“ wird aus Gründen des Sprachgebrauchs in dieser Übersetzung teils mit „technologisch“, teils mit „technisch“ übersetzt. Inhaltlich ist hiermit keine Unterscheidung beabsichtigt.

7 Wörtlich: „Arbeitsaufgaben“.

第七条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

§ 7 [Verhalten im Netzwerk und Förderung der Netzwerksicherheit; = § 6 a. F.] Der Staat setzt sich ein für ein kultiviertes und gesundes Verhalten im Netzwerk nach [den Grundsätzen von] Treu und Glauben, fördert die Verbreitung des Systems der Kernwerte des Sozialismus, ergreift Maßnahmen zur Anhebung der gesamtgesellschaftlichen Kenntnisse und des Niveaus der Netzwerksicherheit [und] schafft ein positives Umfeld zur Beteiligung der gesamten Gesellschaft an der Förderung der Netzwerksicherheit.

第八条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

§ 8 [Internationale Zusammenarbeit, Netzwerkregulierung; = § 7 a. F.] Der Staat führt aktiv den internationalen Austausch und die internationale Zusammenarbeit auf Gebieten wie etwa der Regulierung des Cyberspace, der Forschung und Entwicklung von Netzwerktechnologie, der Festlegung von Standards sowie der Bekämpfung rechtswidriger Straftaten im Netzwerk aus, fördert den Aufbau eines friedlichen, sicheren, offenen, kooperativen Cyberspace [und] errichtet ein multilaterales, demokratisches, transparentes Netzwerkregulierungssystem.

第九条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

§ 9 [Zuständigkeiten; = § 8 a. F.] Die staatlichen Abteilungen für Netzwerke und Informationen[8] verantworten die umfassende Koordinierung der Aufgaben der Netzwerksicherheit und die relevanten Aufgaben der Aufsicht und Verwaltung. Die Abteilungen des Staatsrates für Telekommunikation und Öffentliche Sicherheit und andere betreffende Behörden verantworten jede innerhalb ihrer Amtspflichten den Schutz der Netzwerksicherheit sowie die [entsprechenden] Aufgaben der Verwaltung und Aufsicht gemäß den Bestimmungen dieses Gesetzes, relevanter [anderer] Gesetze und Verwaltungsrechtsnormen[9].

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

Die Amtspflichten der betreffenden Abteilungen der Volksregierungen ab der Kreisebene im Rahmen des Schutzes, der Aufsicht und Verwaltung der Netzwerksicherheit bestimmen sich gemäß den relevanten staatlichen Bestimmungen.

第十条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

§ 10 [Pflichten der Netzwerkbetreiber und gesellschaftliche Verantwortung; = § 9 a. F.] Netzwerkbetreiber, die Geschäfte und Dienstleistungsaktivitäten[10] ausführen, haben die Gesetze und Verwaltungsrechtsnormen zu befolgen, die Sozialmoral zu respektieren, die Geschäftsethik zu befolgen, aufrichtig und vertrauenswürdig [zu handeln], [ihre] Pflichten zum Schutz der Netzwerksicherheit zu erfüllen, sich der Aufsicht durch Regierung und Gesellschaft zu unterwerfen [und] die gesellschaftliche Verantwortung zu tragen.

8 Es dürfte sich hierbei insbesondere um einen Verweis auf die sog. Cyberspace Administration of China (CAC, 国家互联网信息办公室) handeln. Die CAC ist eine Abteilung des Staatsrates und institutionell identisch mit dem „State Council Information Office of the People's Republic of China" (国务院新闻办公室). Auf der Arbeitsebene ist sie mit dem „Office of the Central Cyberspace Affairs Commission"(中共中央网络安全和信息化委员会办公室) eng verbunden. Letztere wiederum ist eine Abteilung des Zentralkomitees der KP China.

9 Die genannten „Verwaltungsrechtsnormen" beziehen sich gemäß § 72 Gesetzgebungsgesetz der Volksrepublik China [中华人民共和国立法法] vom 15.3.2000 in der Fassung vom 13.3.2023 (chinesisch-deutsch in: ZChinR 2023, S. 87 ff.) ausschließlich auf Rechtsakte des Staatsrates.

10 Ausnahmsweise ist hier „服务" als Dienst*leistung* übersetzt. Im Rest des Dokuments wird als „Dienste" übersetzt; die Abweichung wurde hier allein aus Gründen des Sprachflusses gewählt.

第十一条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

§ 11 [Datenschutz; = § 10 a. F.] Wer Netzwerke errichtet oder geschäftlich betreibt oder mittels Netzwerken Dienstleistungen anbietet, muss gemäß den Bestimmungen in Gesetzen und Verwaltungsrechtsnormen sowie den zwingenden Anforderungen nationaler Standards technische oder andere nötige Maßnahmen ergreifen, die Netzwerksicherheit und den stabilen Betrieb gewährleisten, effektiv auf Störfälle der Netzwerksicherheit[11] reagieren, rechtswidrigen kriminellen Netzwerkaktivitäten vorbeugen [und] die Integrität, Geheimhaltung und Nutzbarkeit von Netzwerkdaten bewahren.

第十二条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

§ 12 [Selbstkontrolle der Wirtschaft; = § 11 a. F.] Netzwerkrelevante Branchenorganisationen stärken ihren Satzungen gemäß die Selbstkontrolle der Branche, legen Verhaltensregeln zur Netzwerksicherheit fest, leiten [ihre] Mitglieder an zur Stärkung der Netzwerksicherheit, erhöhen das Niveau der Netzwerksicherheit [und] fördern die gesunde Entwicklung der Branche.

第十三条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

§ 13 [Staatlicher Schutz der Netzwerksicherheit; = § 12 a. F.] Der Staat schützt die Rechte der Bürger, juristischen Personen und anderer Organisationen bei der rechtmäßigen Nutzung von Netzwerken, fördert die Verbreitung des Netzwerkzugangs, erhöht das Niveau an Netzwerkdiensten, stellt der Gesellschaft sichere und bequeme Netzwerkdienste zur Verfügung [und] gewährleistet den rechtmäßigen, geordneten, freien Fluss von Netzwerkinformationen.

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

Jede Person und jede Organisation, die ein Netzwerk nutzt, muss die Verfassung [und] Gesetze befolgen, die öffentliche Ordnung einhalten, die Sozialmoral respektieren, darf nicht die Netzwerksicherheit gefährden [und] darf das Netzwerk nicht dazu gebrauchen, Aktivitäten auszuführen, die etwa die staatliche Sicherheit, das staatliche Ansehen oder Interesse gefährden, zum Umsturz der staatlichen Führung oder zur Umwälzung des sozialistischen Gesellschaftssystems aufwiegeln, zur Spaltung des Staates oder der Zerstörung der staatlichen Einheit aufhetzen, den Terrorismus oder Extremismus anpreisen, Feindschaft, Hass und Diskriminierung bezüglich nationaler Minderheiten anpreisen, Gewalt oder obszöne pornografische Informationen verbreiten, Falschinformationen erstellen oder verbreiten, die die wirtschaftliche oder gesellschaftliche Ordnung stören oder die die Ehre, Privatsphäre, Rechte an geistigem Eigentum oder andere legale Rechte und Interessen einer anderen Person verletzen.

第十四条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

§ 14 [Schutz Minderjähriger; = § 13 a. F.] Der Staat unterstützt Forschung und Entwicklung von Netzwerkprodukten und -diensten zum Nutzen des gesunden Aufwachsens von Minderjährigen, bestraft dem Recht gemäß Aktivitäten, deren Ausführung unter Nutzung eines Netzwerks die körperliche oder geistige Gesundheit eines Minderjährigen gefährden, [und] stellt Minderjährigen eine sichere und gesunde Netzwerkumgebung zur Verfügung.

11 Wörtlich: „Netzwerksicherheitsvorfall“.

第十五条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

§ 15 [Meldung gefährlichen Verhaltens; = § 14 a. F.] Jede Person oder Organisation hat das Recht, über Verhalten, das die Netzwerksicherheit gefährdet, bei den Abteilungen wie etwa der für Netzwerke und Informationen, Telekommunikation oder Öffentliche Sicherheit Meldung zu machen. Die Abteilung, welche die Meldung empfängt, muss [die Angelegenheit] unverzüglich gemäß dem Recht behandeln; gehört diese [Angelegenheit] nicht zu den Amtspflichten dieser Abteilung, muss [sie die Meldung] unverzüglich an die zur Behandlung berechtigte Abteilung weiterleiten.

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益

Die betreffenden Abteilungen müssen die relevanten Informationen der die Meldung machenden Person geheim halten [und] die Rechte und Interessen dieser Person schützen.

第二章 网络安全支持与促进

2. Kapitel: Unterstützung und Förderung der Netzwerksicherheit

第十六条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

§ 16 [Netzwerksicherheitsstandards, Teilhabe an deren Formulierung; = § 15 a. F.] Der Staat erschafft und perfektioniert ein System von Netzwerksicherheitsstandards. Die für Standardisierung zuständige Verwaltungsabteilung des Staatsrates und andere betreffende Abteilungen des Staatsrates organisieren gemäß ihren jeweiligen Amtspflichten die Festlegung betreffender nationaler Standards und Branchenstandards zur Verwaltung der Netzwerksicherheit sowie zur Sicherheit von Netzwerkprodukten, -diensten und -betätigungen sowie die zeitige Revision [dieser Standards].

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

Der Staat unterstützt die Teilnahme von Unternehmen, Forschungseinrichtungen, Hochschulen und netzwerkrelevanten Branchenorganisationen bei der Festlegung nationaler Standards oder von Branchenstandards zur Netzwerksicherheit.

第十七条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

§ 17 [Umfassende Planung aller staatlichen Ebenen; = § 16 a. F.] Der Staatsrat und die Volksregierungen der Provinzen, autonomen Gebiete oder regierungsunmittelbaren Städte müssen eine umfassende Planung auflegen, Investitionen ausweiten, Industriezweigen und Projekten in den Schwerpunktbereichen der Netzwerksicherheitstechnologie Hilfe gewähren, Forschung und Entwicklung sowie Nutzung von Netzwerksicherheitstechnologie unterstützen, vertrauenswürdige und sichere Netzwerkprodukte und Netzwerkdienste verbreiten, das geistige Eigentum an Netzwerktechnologie schützen [und] Unternehmen, Forschungseinrichtungen, Hochschulen und andere bei der Teilnahme an innovativen Projekten der Netzwerksicherheitstechnologie unterstützen.

第十八条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

§ 18 [Dienste zur Einschätzung der Netzwerksicherheit; = § 17 a. F.] Der Staat treibt unter verstärkter Einbeziehung gesellschaftlicher (privater) Akteure[12] den Aufbau eines Systems von Netzwerksicherheitsdiensten voran [und] ermutigt betreffende Unternehmen [und] Einrichtungen, Sicherheitsdienste wie etwa zur Bestätigung, Prüfung oder Risikobewertung der Netzwerksicherheit auszuüben.

12 Wörtlich könnte 社会化 mit „Vergesellschaftung“ übertragen werden. Dies hat im Deutschen allerdings zu sehr den Klang einer „Verstaatlichung“. Hier ist ganz im Gegenteil die verstärkte Einbeziehung Privater gemeint.

第十九条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

§ 19 [Innovationsförderung der Netzwerksicherheit; = § 18 Abs. 1 a. F.] Der Staat ermutigt die Entwicklung von Technologie zum Schutz der Sicherheit und zur Nutzung von Netzwerkdaten, fördert die Öffnung öffentlicher Datenressourcen [und] fördert technologische Innovationen und die sozioökonomische Entwicklung.

第二十条 国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

§ 20 [Förderung der Grundlagenforschung zu Künstlicher Intelligenz, Innovationsförderung der Netzwerkverwaltung; Abs. 1 neu eingefügt, Abs. 2 vgl. § 18 Abs. 2 a. F.] Der Staat unterstützt die Grundlagenforschung zu Künstlicher Intelligenz sowie die Forschung und Entwicklung zentraler Technologien wie etwa Algorithmen, treibt den Aufbau von Infrastrukturen wie etwa Trainingsdatenressourcen und Rechenleistung voran, vervollkommnet die ethischen Normen für Künstliche Intelligenz, stärkt die Überwachung und Bewertung von Risiken sowie die Sicherheitsaufsicht und fördert die Anwendung und gesunde Entwicklung von Künstlicher Intelligenz.

国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

Der Staat unterstützt innovative Methoden der Netzwerksicherheitsverwaltung, wendet neue Technologien wie Künstliche Intelligenz an und steigert das Niveau des Schutzes der Netzwerksicherheit.

第二十一条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

§ 21 [Aufklärungsarbeit zur Netzwerksicherheit; Massenmedien; = § 19 a. F.] Die Volksregierungen aller Ebenen sowie deren betreffende Abteilungen müssen die Durchführung regelmäßiger Öffentlichkeitsarbeit[13] zur Netzwerksicherheit organisieren und die betreffenden Einheiten zu guter Öffentlichkeitsarbeit anleiten und anhalten.

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

Die Massenmedien müssen auf die Gesellschaft zielgerichtete Öffentlichkeitsarbeit zur Netzwerksicherheit durchführen.

第二十二条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

§ 22 [Förderung qualifizierten Personals; = § 20 a. F.] Der Staat unterstützt Unternehmen und Bildungs- oder Schulungseinrichtungen wie Hochschulen, Berufsschulen bei der Durchführung relevanter Bildung oder Schulung zur Netzwerksicherheit [und] wendet eine Vielzahl von Methoden zur Heranbildung qualifizierten Personals in der Netzwerksicherheit an und fördert den Austausch qualifizierten Personals in der Netzwerksicherheit.

第三章 网络运行安全

3. Kapitel: Funktionssicherheit von Netzwerken

第一节 一般规定

1. Abschnitt: Allgemeine Bestimmungen

第二十三条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改

§ 23 [Mehrstufiges Schutzsystem; = § 21 a. F.] Der Staat implementiert ein mehrstufiges Schutzsystem der Netzwerksicherheit. Netzwerkbetreiber müssen gemäß der Erfordernisse dieses mehrstufigen Schutzsystems der Netzwerksicherheit die folgenden Sicherheitsschutzpflichten erfüllen und gewährleisten, dass Störungen des Netzwerks, Zerstörung oder unbefugte Zugriffe[14] vermieden [und so] Datenlecks oder Diebstahl oder Fälschung verhindert werden:

13 Wörtlich: „Propaganda [und] Erziehung“.

14 Wörtlich: „Besuchen“.

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

1. Festlegung eines internen Sicherheitsverwaltungssystems und von Durchführungsbestimmungen, Festlegung eines Verantwortlichen für die Netzwerksicherheit, Umsetzung der Verpflichtungen zum Schutz der Netzwerksicherheit;

2. Ergreifen technologischer Maßnahmen zur Prävention gegen Computerviren und die Sicherheit des Netzwerks gefährdenden Verhaltens wie etwa Netzwerkangriffe oder das Eindringen ins Netzwerk;

3. Ergreifen technologischer Maßnahmen zur Überwachung [und] Aufzeichnung des Funktionszustands des Netzwerks [und] von Störfällen der Netzwerksicherheit[15] sowie den Bestimmungen gemäß die Speicherung relevanter Netzwerkprotokolle der zumindest letzten sechs Monate;

4. Ergreifen von Maßnahmen wie der Klassifizierung von Daten, der Sicherung wichtiger Daten und der Verschlüsselung;

5. andere in Gesetzen oder Verwaltungsrechtsnormen bestimmte Pflichten.

第二十四条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

§ 24 [Schutzpflichten der Anbieter von Netzwerkprodukten und -diensten, dauerhafter Schutz, Einverständnis von Nutzern; = § 22 a. F.] Netzwerkprodukte oder -dienste müssen den zwingenden Anforderungen relevanter nationaler Standards genügen. Die Anbieter von Netzwerkprodukten oder -diensten dürfen keine Malware[16] installieren; entdecken sie an ihren Netzwerkprodukten oder -diensten Risiken wie Sicherheitsmängel oder -lücken, so müssen sie sofort Hilfsmaßnahmen ergreifen, den Bestimmungen gemäß unverzüglich die Nutzer benachrichtigen sowie der betreffenden zuständigen Abteilung Bericht erstatten.

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

Anbieter von Netzwerkprodukten oder -diensten müssen bezüglich ihrer Netzwerkprodukte oder -dienste dauerhaften Sicherheitsschutz zur Verfügung stellen; innerhalb der in Bestimmungen oder einer Parteivereinbarung [hierfür] vorgesehenen Zeitspanne darf die Zurverfügungstellung des Sicherheitsschutzes nicht beendet werden.

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

Enthalten Netzwerkprodukte oder -dienste Funktionen zur Sammlung von Nutzerdaten, so müssen deren Anbieter Nutzer ausdrücklich [darauf] hinweisen und ihr Einverständnis [hierzu] einholen[17]; soweit es um persönliche Informationen der Nutzer geht, müssen zudem die Bestimmungen dieses Gesetzes sowie betreffender [anderer] Gesetze und Verwaltungsrechtsnormen zum Schutz persönlicher Informationen befolgt werden.

15 Siehe Fn. 11.

16 Wörtlich: „bösartige Programme“.

17 Wörtlich: „erlangen“.

第二十五条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

§ 25 [Sicherheitsbestätigung und -evaluierung; = § 23 a. F.] Wesentliche Netzwerkausstattung und spezielle Netzwerksicherheitsprodukte dürfen gemäß den zwingenden Anforderungen relevanter nationaler Standards erst nach Bestätigung der Sicherheitskonformität durch eine qualifizierte Einrichtung oder einer den Anforderungen entsprechenden Prüfung verkauft oder angeboten werden. Die staatlichen Abteilungen für Netzwerke und Informationen formulieren zusammen mit den betreffenden Abteilungen des Staatsrates einen Katalog wesentlicher Netzwerkausstattung und spezialisierter Netzwerksicherheitsprodukte und geben [diesen] bekannt und fördern die gegenseitige Anerkennung von Sicherheitsbestätigungen und der Ergebnisse von Sicherheitsevaluierungsergebnissen [und] vermeiden mehrfache Bestätigungen und Evaluierungen.

第二十六条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

§ 26 [Authentifizierung, staatliche Glaubwürdigkeitsstrategie; = § 24 a. F.] Netzwerkbetreiber, die für ihre Kunden den Netzwerkzugang oder Dienste der Domainnamenregistrierung erledigen, die Formalitäten des Netzzugangs per Festnetz- oder Mobiltelefon erledigen oder ihren Kunden Dienste wie etwa das Veröffentlichen von Informationen oder das Echtzeitchatten zur Verfügung stellen, müssen von dem Kunden entweder bei Unterzeichnung einer Vereinbarung mit dem Kunden oder bei Bestätigung der Zurverfügungstellung des Dienstes die Zurverfügungstellung von Informationen über seine wahre Identität verlangen. Stellt der Kunde keine Informationen über seine wahre Identität zur Verfügung, so darf der Netzwerkbetreiber diesem nicht die betreffenden Dienste zur Verfügung stellen.

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认

Der Staat implementiert eine Strategie zur Glaubwürdigkeit von Netzwerkidentitäten, unterstützt Forschung und Entwicklung von sicheren [und] benutzerfreundlichen[18] Technologien zur elektronischen Identitätsbestätigung [und] fördert die gegenseitige Anerkennung zwischen unterschiedlichen elektronischen Identitätsbestätigungen.

第二十七条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

§ 27 [Notfallplan; = § 25 a. F.] Netzwerkbetreiber müssen einen Notfallplan für Netzwerksicherheitsstörfälle[19] festlegen [und] unverzüglich Sicherheitsrisiken wie etwa Systemanfälligkeiten[20], Computerviren, Netzwerkangriffe [oder] ein Eindringen ins Netzwerk handhaben; ereignet sich ein die Netzwerksicherheit gefährdender Störfall, [so] wird sofort der Notfallplan gestartet, werden die entsprechenden Abhilfemaßnahmen ergriffen und den Bestimmungen gemäß der betreffenden zuständigen Abteilung Bericht erstattet.

18 Wörtlich: „bequemen/angenehmen/einfachen“.

19 Siehe Fn. 11.

20 Wörtlich: „Systemlücken“.

第二十八条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

§ 28 [Veröffentlichung von Netzwerksicherheitsinformationen; = § 26 a. F.] Aktivitäten wie die Durchführung von Bestätigungen, Prüfungen [oder] Risikobewertungen der Netzwerksicherheit [sowie ebenfalls] die Veröffentlichung[21] von Netzwerksicherheitsinformationen wie etwa zu Systemanfälligkeiten, Computerviren, Netzwerkangriffen [oder] dem Eindringen ins Netzwerk müssen gemäß den betreffenden Bestimmungen des Staates erfolgen[22].

第二十九条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

§ 29 [Verbot der Gefährdung der Netzwerksicherheit; = § 27 a. F.] Keine Person oder Organisation darf Aktivitäten ausführen, welche die Netzwerksicherheit gefährden, wie etwa das illegale Eindringen in ein fremdes Netzwerk[23], die Störung der normalen Funktion[stüchtigkeit] eines fremden Netzwerks [oder] der Diebstahl von Netzwerkdaten; es dürfen keine die Netzwerksicherheit gefährdenden Programme oder Werkzeuge zur Verfügung gestellt werden, die speziell zum Eindringen in Netzwerke, zur Störung der normalen Funktion[stüchtigkeit] eines Netzwerks [oder der Störung] von Schutzmaßnahmen [oder] dem Diebstahl von Netzwerkdaten genutzt[24] werden; gibt es klare Kenntnis über die Netzwerksicherheit gefährdende Aktivitäten anderer Personen, [so] dürfen diesen keine Hilfe wie etwa durch technologische Unterstützung, durch Inumlaufbringen von Werbung oder bei der Abwicklung von Zahlungen zur Verfügung gestellt werden.

第三十条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

§ 30 [Pflicht zur Unterstützung der Sicherheitsbehörden durch die Betreiber; = § 28 a. F.] Netzwerkbetreiber müssen die Behörden für öffentliche Sicherheit und die staatlichen Sicherheitsbehörden[25] bei der rechtmäßigen Wahrung der staatlichen Sicherheit und der Ermittlung von kriminellen Aktivitäten technologische Unterstützung und Hilfe zur Verfügung stellen.

第三十一条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

§ 31 [Zusammenarbeit von Netzwerkbetreibern, Pflichten von Branchenorganisationen; = § 29 a. F.] Der Staat unterstützt die Zusammenarbeit[26] zwischen den Netzwerkbetreibern in Bereichen wie etwa der Sammlung [oder] Analyse von [oder] des Berichts über Netzwerksicherheitsinformationen sowie der Handhabung von Notfällen, [um] die Fähigkeiten der Netzwerkbetreiber zur Gewährleistung von Sicherheit zu erhöhen.

21 Wörtlich: „Veröffentlichung gegenüber der Gesellschaft“.

22 Wörtlich: „müssen die betreffenden Bestimmungen ... befolgen“.

23 Wörtlich: „Netzwerk einer anderen Person“.

24 Wörtlich: „zur Ausführung des Eindringens ... genutzt werden“.

25 Sowohl die Behörden für öffentliche Sicherheit (公安机关) als auch die staatlichen Sicherheitsbehörden (国家安全机关) sind Verwaltungsbehörden, die für die Ermittlung unrechtmäßigen Verhaltens zuständig sind. Sie unterscheiden sich allerdings in ihren Aufgaben: Die Hauptaufgabe der staatlichen Sicherheitsbehörden ist die Wahrung der Staatssicherheit, etwa durch die Verhinderung von Straftaten wie der Spionage oder anderer schwerwiegender Aktivitäten. Die Behörden für öffentliche Sicherheit sind zuständig für die Verhinderung und Ermittlung bezüglich anderer, geringschwelligerer krimineller Aktivitäten.

26 Wörtlich: „Die Eingehung/Durchführung von Zusammenarbeit“.

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

Betreffende Branchenorganisationen führen starke Branchenregularien zum Schutz der Netzwerksicherheit und einen Koordinationsmechanismus ein, stärken die Analyse und Bewertung der Netzwerksicherheit, führen ihren Mitgliedern gegenüber regelmäßig Sicherheitswarnungen durch [und] unterstützen und helfen Mitgliedern dabei, Netzwerksicherheitsrisiken entgegenzutreten.

第三十二条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

§ 32 [Schutz erlangter Informationen; = § 30 a. F.] Informationen, welche die Abteilungen für Netzwerke und Informationen und betreffende Abteilungen bei Erfüllung ihrer Amtspflichten zum Schutz der Netzwerksicherheit erlangen, dürfen nur für die [Erfüllung der] Erfordernisse der Wahrung der Netzwerksicherheit genutzt werden, nicht [aber] zu anderen Zwecken.

第二节 关键信息基础设施的运行安全

2. Abschnitt: Funktionssicherheit wesentlicher Informationsinfrastruktur

第三十三条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

§ 33 [Schwerpunktschutz; = § 31 a. F.] Der Staat vollzieht auf Grundlage des mehrstufigen Schutzsystems[27] den schwerpunktmäßigen Schutz wichtiger Branchen und Bereiche wie etwa öffentlicher Kommunikations- und Informationsdienste, Energieressourcen, Verkehrswesen, Wasserwirtschaft, Finanzwesen, öffentlicher Dienste, elektronischer Verwaltung sowie anderer essenzieller Informationsinfrastruktur, die im Falle plötzlicher Zerstörung[28], Funktionseinbuße oder von Datenlecks die staatliche Sicherheit, die Finanzverwaltung des Staates und die Lebenshaltung der Bevölkerung oder das öffentliche Interesse schwerwiegend gefährden kann. Der genaue Umfang und die [genaue] Art und Weise des Sicherheitsschutzes wesentlicher Informationsinfrastruktur wird vom Staatsrat festgelegt.

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

Der Staat ermutigt Netzwerkbetreiber, [in Bereichen] außerhalb wesentlicher Informationsinfrastruktur freiwillig an dem System des Schutzes wesentlicher Informationsinfrastruktur teilzunehmen.

第三十四条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

§ 34 [Sicherheitspläne zum Schutz wesentlicher Informationsinfrastruktur; = § 32 a. F.] Die gemäß der durch den Staatsrats bestimmten Zuteilung von Amtspflichten für die Aufgabe des Sicherheitsschutzes wesentlicher Informationsinfrastruktur verantwortlichen Abteilungen verfassen und organisieren separat die Implementierung der Sicherheitsplanung bezüglich der wesentlichen Informationsinfrastruktur der jeweiligen[29] Branche oder des jeweiligen Bereichs und leiten und beaufsichtigen die Arbeiten zum Schutz der Sicherheit beim Betrieb wesentlicher Informationsinfrastruktur.

27 Siehe § 23.

28 Wörtlich: „bei plötzlichem Erleiden von Zerstörung“.

29 Wörtlich: „*dieser* Branche“. Gemeint ist wohl die in den jeweiligen Aufgabenbereich der fraglichen Abteilungen fallende Branche.

第三十五条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

§ 35 [Sicherheitsschutz beim Aufbau wesentlicher Informationsinfrastruktur; = § 33 a. F.] Beim Aufbau wesentlicher Informationsinfrastruktur muss deren Funktionsfähigkeit zur Unterstützung stabiler geschäftlicher Tätigkeit und dauerhaften Betriebs gewährleistet werden und garantiert werden, dass Maßnahmen der Sicherheitstechnologie im Gleichlauf geplant, ins Werk gesetzt und genutzt werden.

第三十六条 除本法第二十三条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

§ 36 [Zusätzliche Pflichten der Betreiber wesentlicher Informationsinfrastruktur; = § 34 a. F.] Außer der Bestimmungen in § 23 dieses Gesetzes müssen die Betreiber wesentlicher Informationsinfrastruktur [zusätzlich] die folgenden Sicherheitsschutzpflichten erfüllen:

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

1. Einsetzung eines speziellen Sicherheitsverwaltungsorgans und einer für das Sicherheitsmanagement verantwortlichen Person und Durchführung der Überprüfung des sicherheitsrelevanten Hintergrunds[30] dieser verantwortlichen Person und des Personals auf Schlüsselpositionen;

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

2. Durchführung regelmäßiger Bildung[sveranstaltungen] zur Netzwerksicherheit, technologischer Schulung und testweiser Überprüfung der technischen Fähigkeiten des Personals;

（三）对重要系统和数据库进行容灾备份；

3. Durchführung von Notfallsicherungen bezüglich wichtiger Systeme und Datenbanken;

（四）制定网络安全事件应急预案，并定期进行演练；

4. Festlegung eines Notfallplans für Störfälle der Netzwerksicherheit[31] und die regelmäßige Durchführung von Übungen;

（五）法律、行政法规规定的其他义务。

5. andere in Gesetzen und Verwaltungsrechtsnormen bestimmte Pflichten.

第三十七条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

§ 37 [Sicherheitstests potenziell gefährlicher Netzwerkprodukte und -dienste; = § 35 a. F.] Erwerben die Betreiber wesentlicher Informationsinfrastruktur Netzwerkprodukte oder -dienste, welche die staatliche Sicherheit beeinträchtigen können, so müssen diese die von den staatlichen Abteilungen für Netzwerke und Informationen zusammen mit den betreffenden Abteilungen des Staatsrates organisierten Sicherheitstests durchlaufen.

第三十八条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任

§ 38 [Sicherheits- und Verschwiegenheitsvereinbarungen; = § 36 a. F.] Erwerben die Betreiber wesentlicher Informationsinfrastruktur Netzwerkprodukte oder -dienste, [so] müssen sie den Bestimmungen gemäß mit den Anbietern Sicherheits- und Verschwiegenheitsvereinbarungen unterzeichnen [und darin] die Pflichten und Verantwortlichkeiten der Sicherheit und Verschwiegenheit deutlich benennen.

30 Wörtlich: „Sicherheitshintergrund“.

31 Siehe Fn. 11.

第三十九条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

§ 39 [Persönliche Daten, inländische Speicherpflicht; = § 37 a. F.] Persönliche Informationen und wichtige Daten, die Betreiber wesentlicher Informationsinfrastruktur innerhalb des Gebiets der Volksrepublik China sammeln und erstellen, müssen innerhalb des Gebiets [der Volksrepublik China] gespeichert werden. Ist es aufgrund der Erfordernisse der geschäftlichen Tätigkeit wirklich erforderlich, [Informationen und Daten] außerhalb des Gebiets [der Volksrepublik China] zur Verfügung zu stellen, [so] müssen sie gemäß der von den staatlichen Abteilungen für Netzwerke und Informationen zusammen mit den betreffenden Abteilungen des Staatsrates festgelegten Art und Weise Sicherheitsbewertungen durchführen. Enthalten Gesetze oder Verwaltungsrechtsnormen anderweitige Bestimmungen, so gelten diese Bestimmungen.

第四十条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

§ 40 [Jährliche Prüfung; = § 38 a. F.] Die Betreiber wesentlicher Informationsinfrastruktur müssen zumindest einmal pro Jahr selbsttätig oder mittels Beauftragung einer Einrichtung für Netzwerksicherheitsdienste eine Prüfung und Bewertung der Sicherheit und der potenziell bestehenden Risiken in ihrem Netzwerk durchführen und [müssen] die Ergebnisse[32] der Prüfung und Bewertung sowie Verbesserungsmaßnahmen an die relevanten, für den Schutz der Sicherheit[33] wesentlicher Informationsinfrastruktur verantwortlichen Abteilungen berichten.

第四十一条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

§ 41 [Koordinierung des Schutzes; = § 39 a. F.] Die staatlichen Abteilungen für Netzwerke und Informationen müssen den Schutz der Sicherheit wesentlicher Informationsinfrastruktur durch die relevanten Abteilungen unter Ergreifung der folgenden Maßnahmen umfassend koordinieren:

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估

1. stichprobenartig die Prüfung des Sicherheitsrisikos wesentlicher Informationsinfrastruktur ausführen, Verbesserungsmaßnahmen vorgeben, nötigenfalls eine Einrichtung für Netzwerksicherheitsdienste mit der Ausführung der Prüfung und Bewertung von bestehenden Netzwerksicherheitsrisiken beauftragen;

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

2. regelmäßig die Ausführung von Notfallübungen zur Netzwerksicherheit durch die Betreiber wesentlicher Informationsinfrastruktur organisieren [und] das Niveau sowie die Fähigkeit zu koordinierter Zusammenarbeit bei der Reaktion auf Störfalle der Netzwerksicherheit[34] erhöhen;

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

3. den Austausch von Netzwerksicherheitsinformationen fördern zwischen beispielsweise den betreffenden Abteilungen, den Betreibern wesentlicher Informationsinfrastruktur und den betreffenden Forschungseinrichtungen sowie Einrichtungen für Netzwerksicherheitsdienste;

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

4. technische Unterstützung und Hilfe zur Verfügung stellen bezüglich beispielsweise der Notfallhandhabung von Störfällen der Netzwerksicherheit und der Wiederherstellung der Netzwerkfunktion.

32 Wörtlich: „die Situation/Umstände der Prüfung ...“.

33 Wörtlich: „für die Aufgabe des Schutzes der Sicherheit“.

34 Siehe Fn. 11.

第四章　网络信息安全

第四十二条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

第四十三条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十四条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

4. Kapitel: Sicherheit von Netzwerkinformationen

§ 42 [Schutz von Nutzerinformationen; Abs. 1 = § 40 a. F., Abs. 2 neu eingefügt] Netzwerkbetreiber müssen gesammelte Nutzerinformationen streng geheim halten [und] ein starkes System zum Schutz der Nutzerinformationen aufbauen.

Netzwerkbetreiber müssen bei der Behandlung persönlicher Informationen die Bestimmungen dieses Gesetzes sowie die des „Zivilgesetzbuches der Volksrepublik China“[35] und des „Gesetzes der Volksrepublik China zum Schutz persönlicher Daten“[36] und anderer Gesetze und Verwaltungsrechtsnormen befolgen.

§ 43 [Sammlung persönlicher Informationen, dienstfremde Informationen; = § 41 a. F.] Netzwerkbetreiber, die persönliche Informationen sammeln und nutzen, müssen die Prinzipien der Rechtmäßigkeit, Fairness und Notwendigkeit befolgen, die Regeln der Sammlung und Nutzung offenlegen, ausdrücklich auf den Zweck, die Art und Weise sowie den Umfang der Sammlung und Nutzung der Informationen hinweisen und das Einverständnis der Nutzer[37] einholen.

Netzwerkbetreiber dürfen keine persönlichen Informationen sammeln, die in keinem Zusammenhang zu den von ihnen erbrachten Diensten stehen, dürfen nicht unter Verstoß gegen Bestimmungen in Gesetzen oder Verwaltungsrechtsnormen oder beiderseitigen Vereinbarungen persönliche Informationen sammeln oder nutzen und müssen die von ihnen gespeicherten persönlichen Informationen gemäß den Bestimmungen in Gesetzen [oder] Verwaltungsrechtsnormen und der Vereinbarung mit dem Nutzer behandeln.

§ 44 [Verbot von Preisgabe, Verfälschung oder Vernichtung, Maßnahmen der Wiedergutmachung; = § 42 a. F.] Netzwerkbetreiber dürfen die von ihnen gesammelten persönlichen Informationen nicht preisgeben, verfälschen oder vernichten; ohne das Einverständnis des Nutzers dürfen sie persönliche Informationen nicht Dritten zur Verfügung stellen, es sei denn, die Zuordnung zu einer bestimmten Person wurde durch Anonymisierung aufgehoben[38] und kann auch nicht wiederhergestellt werden.

Netzwerkbetreiber müssen technische und andere nötige Maßnahmen ergreifen, [um] die Sicherheit der von ihnen gesammelten persönlichen Informationen zu gewährleisten, [und] verhindern, dass Informationen preisgegeben, vernichtet oder verloren werden. Im Falle der eingetretenen oder möglichen Preisgabe, Vernichtung oder des Verlusts persönlicher Informationen müssen sofort Maßnahmen zur Wiedergutmachung ergriffen, die Nutzer den Bestimmungen gemäß unverzüglich benachrichtigt werden und [es muss] gegenüber den betreffenden zuständigen Abteilungen Bericht erstattet werden.

35 Chinesisch-deutsch abgedruckt in: ZChinR 2020, S. 207 ff.

36 Chinesisch-deutsch abgedruckt in: ZChinR 2021, S. 286 ff.

37 Wörtlich: „derjenigen, die das Objekt der Sammlung sind“.

38 Wörtlich: „[die Informationen] wurden so behandelt, dass bestimmte Personen unkenntlich sind“.

第四十五条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

§ 45 [Recht auf Löschung oder Korrektur persönlicher Informationen; = § 43 a. F.] Bemerkt eine Person, dass ein Netzwerkbetreiber unter Verstoß gegen Bestimmungen in Gesetzen oder Verwaltungsrechtsnormen oder in beiderseitigen Vereinbarungen persönliche Informationen dieser Person sammelt oder nutzt, so hat sie das Recht, vom Netzwerkbetreiber die Löschung der persönlichen Informationen zu verlangen; bemerkt sie, dass die gesammelten und gespeicherten persönlichen Daten fehlerhaft sind, so hat sie das Recht, vom Netzwerkbetreiber die Korrektur [der Informationen] zu verlangen. Der Netzwerkbetreiber muss [auf ein solches Verlangen hin] Maßnahmen zur Löschung oder Korrektur ergreifen.

第四十六条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

§ 46 [Verbot rechtswidriger Erlangung von Informationen und rechtswidrigen Handels; = § 44 a. F.] Keine Person oder Organisation darf persönliche Informationen stehlen oder auf andere illegale Weise erlangen [und] darf persönliche Informationen nicht illegal verkaufen oder illegal Dritten zur Verfügung stellen.

第四十七条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

§ 47 [Geheimhaltungspflicht staatlicher Abteilungen; = § 45 a. F.] Die gesetzlich für die Aufsicht und Verwaltung der Netzwerksicherheit verantwortlichen[39] Abteilungen und deren Mitarbeiter haben die ihnen bei Erfüllung ihrer Amtspflichten zur Kenntnis gelangten persönlichen Informationen, privaten Informationen und Geschäftsgeheimnisse streng geheim zu halten [und] dürfen [diese] nicht preisgeben, verkaufen oder illegal Dritten zur Verfügung stellen.

第四十八条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

§ 48 [Verantwortlichkeit für Inhalte von Internetseiten und Gruppenkommunikationen; = § 46 a. F.] Jede Person oder Organisation trägt die Verantwortung[40] für ihr Verhalten bei der Netzwerknutzung, darf keine Internetseite oder Gruppenkommunikation errichten, die dazu genutzt wird, rechtswidrige kriminelle Aktivitäten wie etwa Betrug [oder] die Weitergabe krimineller Methoden [oder] die Herstellung oder den Verkauf verbotener oder [bezüglich Herstellung und Verkauf] beschränkter Gegenstände vorzunehmen [und] darf kein Netzwerk dazu nutzen, Informationen bezüglich Betrugs [oder] der Weitergabe krimineller Methoden [oder] der Herstellung oder des Verkaufs verbotener oder [bezüglich Herstellung und Verkauf] beschränkter Gegenstände oder anderer rechtswidriger krimineller Aktivitäten zu veröffentlichen.

第四十九条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

§ 49 [Beseitigungspflicht der Netzwerkbetreiber; = § 47 a. F.] Netzwerkbetreiber müssen die Verwaltung der von ihren Nutzern veröffentlichten Informationen stärken, müssen, wenn sie Informationen bemerken, deren Veröffentlichung oder Übertragung in Gesetzen oder Verwaltungsrechtsnormen verboten ist, unverzüglich die Übertragung dieser Informationen stoppen, Maßnahmen zur Handhabung wie etwa zur Beseitigung [der Informationen] ergreifen, die Ausbreitung [der Informationen] verhindern, betreffende Aufzeichnungen speichern und der betreffenden zuständigen Abteilung Bericht erstatten.

39 Wörtlich: „die für ... Amtspflichten ... Verantwortlichen“.

40 Wörtlich: „muss die Verantwortung tragen“.

第五十条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

§ 50 [Malware, Gegenmaßnahmen; = § 48 a. F.] Keine von einer Person oder Organisation gesendete elektronische Nachricht oder zur Verfügung gestellte Software darf Malware installieren oder Informationen enthalten, deren Veröffentlichung oder Übertragung Gesetze oder Verwaltungsrechtsnormen verbieten.

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

Anbieter von Diensten zur Sendung elektronischer Nachrichten und Anbieter von Diensten zum Herunterladen von Software müssen Sicherheitsverwaltungspflichten erfüllen [und] müssen, wenn ihnen ein im vorangehenden Absatz beschriebenes Nutzerverhalten bekannt ist, die Zurverfügungstellung der Dienste stoppen, Maßnahmen zur Handhabung wie etwa zur Beseitigung [der Informationen] ergreifen, betreffende Aufzeichnungen speichern und der betreffenden zuständigen Abteilung Bericht erstatten.

第五十一条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

§ 51 [Beschwerde- und Anzeigesystem, Kooperationspflicht; = § 49 a. F.] Netzwerkbetreiber müssen ein Beschwerde- und Anzeigesystem zur Sicherheit von Netzwerkinformationen aufbauen, Informationen etwa über Art und Weise der Beschwerde oder Anzeige bekannt geben [und] unverzüglich Beschwerden und Anzeigen zur Sicherheit von betreffenden Netzwerkinformationen annehmen und bearbeiten.

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

Netzwerkbetreiber müssen mit den Abteilungen für Netzwerke und Informationen und den betreffenden Abteilungen bei der nach dem Gesetz vorgenommenen Aufsicht und Untersuchung zusammenarbeiten.

第五十二条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

§ 52 [Anordnungen zum Stopp der Verbreitung von Informationen; = § 50 a. F.] Wenn Abteilungen für Netzwerke und Informationen oder betreffende Abteilungen in rechtmäßiger Erfüllung ihrer Amtspflicht zur Aufsicht und Verwaltung Informationen bemerken, deren Veröffentlichung oder Übermittlung Gesetze oder Verwaltungsrechtsnormen verbieten, müssen sie von den Netzwerkbetreibern verlangen, die Übertragung zu stoppen, Maßnahmen zur Handhabung wie etwa zur Beseitigung [der Informationen] zu ergreifen [und] betreffende Aufzeichnungen zu speichern; bezüglich Informationen, die von außerhalb des Gebiets der Volksrepublik China stammen, müssen die betreffenden Einrichtungen zur Ergreifung technischer Maßnahmen und anderer nötiger Maßnahmen zum Blockieren der Verbreitung benachrichtigt werden.

第五章监测预警与应急处置

5. Kapitel: Überwachung, Frühwarnung und Handhabung von Notfällen

第五十三条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

§ 53 [Überwachungs- und Frühwarnsystem; = § 51 a. F.] Der Staat baut ein System der Überwachung und Frühwarnung sowie der Informationsweitergabe auf. Die staatlichen Abteilungen für Netzwerke und Informationen müssen die Arbeit der betreffenden Abteilungen zur Sammlung, Analyse und Weitergabe von Netzwerksicherheitsinformationen umfassend koordinieren [und] den Bestimmungen gemäß Überwachungs- und Frühwarninformationen zur Netzwerksicherheit einheitlich veröffentlichen.

第五十四条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

§ 54 [Branchenspezifischer Aufbau; = § 52 a. F.] Die Abteilungen, welche die Aufgabe des Sicherheitsschutzes wesentlicher Informationsinfrastruktur verantworten, müssen ein starkes System der Überwachung und Frühwarnung sowie der Informationsweitergabe in der jeweiligen Branche [oder] dem jeweiligen Bereich aufbauen und den Bestimmungen gemäß über Informationen der Überwachung und Frühwarnung zur Netzwerksicherheit berichten.

第五十五条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

§ 55 [Koordinierung, Notfallpläne, Klassifizierung von Störfällen; = § 53 a. F.] Die staatlichen Abteilungen für Netzwerke und Informationen koordinieren den Aufbau einer starken Risikoanalyse der Netzwerksicherheit und von Arbeitsmechanismen für Notfälle durch die betreffenden Abteilungen, legen Notfallpläne für Netzwerksicherheitsstörfälle[41] fest und organisieren regelmäßige Übungen.

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

Die Abteilungen, welche die Aufgabe des Sicherheitsschutzes wesentlicher Informationsinfrastruktur verantworten, müssen für die jeweilige Branche oder den jeweiligen Bereich Notfallpläne für Netzwerksicherheitsstörfälle festlegen und regelmäßige Übungen organisieren.

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

Notfallpläne für Netzwerksicherheitsstörfälle müssen nach Eintritt des Störfalls gemäß den Faktoren wie etwa des Grads der Gefährdung und des Einflussbereichs eine Klassifizierung der Netzwerksicherheitsstörfälle durchführen und entsprechende Maßnahmen zur Handhabung des Notfalls bestimmen.

第五十六条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

§ 56 [Erhöhtes Risiko von Störfällen; = § 54 a. F.] Ist das Risiko des Eintritts eines Netzwerksicherheitsstörfalls[42] erhöht, so müssen die betreffenden Abteilungen der Volksregierungen ab der Provinzebene[43] gemäß den festgelegten Befugnissen und Verfahren und unter Berücksichtigung der Besonderheiten der Risiken der Netzwerksicherheit und der potenziell eintretenden Gefährdungen die folgenden Maßnahmen ergreifen:

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

1. verlangen, dass die relevanten Abteilungen, Einrichtungen [oder] Mitarbeiter betreffende Informationen sammeln und [über diese] berichten, [und so] die Überwachung des Netzwerksicherheitsrisikos stärken;

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

2. organisieren, dass die betreffenden Abteilungen, Einrichtungen und Fachpersonal Analysen und Bewertungen der Netzwerksicherheitsrisiken durchführen [und] die Wahrscheinlichkeit des Eintritts, Einflussbereichs und Grads der Gefährdung eines Störfalls prognostizieren;

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

3. Frühwarnungen zur Netzwerksicherheit veröffentlichen[44] und Maßnahmen zur Vermeidung und Reduzierung der Gefährdung bekannt geben.

41 Siehe Fn. 11.

42 Siehe Fn. 11.

43 Gemeint sind Abteilungen auf Provinzebene und höherer Ebene.

44 Siehe Fn. 21.

第五十七条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

§ 57 [Vorgehen bei Störfällen; = § 55 a. F.] Im Falle des Eintritts eines Störfalls der Netzwerksicherheit[45] müssen sofort die Notfallpläne bei Störfällen der Netzwerksicherheit ausgeführt werden, es muss eine Untersuchung und Bewertung des Netzwerksicherheitsstörfalls durchgeführt werden, [es muss] von den Netzwerkbetreibern verlangt werden, technische Maßnahmen und andere notwendige Maßnahmen zu ergreifen, latente Gefahren zu beseitigen, die Ausweitung der Gefährdung zu verhindern und unverzüglich die die Öffentlichkeit betreffenden Informationen zur Warnung zu veröffentlichen.[46]

第五十八条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

§ 58 [Vorladung gesetzlicher Repräsentanten und Hauptverantwortlicher; = § 56 a. F.] Bemerken die betreffenden Abteilungen der Volksregierungen ab der Provinzebene bei der Erfüllung ihrer Amtspflichten zur Aufsicht und Verwaltung der Netzwerksicherheit in einem Netzwerk das Bestehen von verhältnismäßig großen Sicherheitsrisiken oder ereignet sich ein Sicherheitsstörfall der Netzwerksicherheit, können sie gemäß der festgelegten Befugnisse und Verfahren den gesetzlichen Repräsentanten oder Hauptverantwortlichen dieses Netzwerkbetreibers zum Gespräch bitten. Der Netzwerkbetreiber muss gemäß der Aufforderung[47] Maßnahmen ergreifen, Änderungen ausführen und die latente Gefahr beseitigen.

第五十九条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

§ 59 [Plötzliche Störfälle und Produktionssicherheitsunfälle; = § 57 a. F.] Tritt aufgrund eines Störfalls der Netzwerksicherheit[48] ein Notfall oder ein Produktionssicherheitsunfall auf, so muss dies gemäß dem „Notfallreaktionsgesetz der Volksrepublik China“[49], dem „Gesetz der Volksrepublik China zur Sicherheit der Produktion“[50] und weiteren betreffenden Bestimmungen in Gesetzen oder Verwaltungsrechtsnormen gehandhabt werden.

第六十条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

§ 60 [Vorübergehende Beschränkungen der Netzwerkkommunikation; = § 58 a. F.] Zur Wahrung der staatlichen Sicherheit und der gesellschaftlichen öffentlichen Ordnung [und] anhand der Erfordernisse der Handhabung eines großen plötzlichen Störfalls können nach Beschluss oder Genehmigung des Staatsrates in bestimmten Gebieten vorübergehend Maßnahmen wie etwa eine Beschränkung der Netzwerkkommunikation ergriffen werden.

45 Siehe Fn. 11.

46 Siehe Fn. 21.

47 Gemeint ist wohl eine in dem in Satz 1 der Vorschrift angesprochenen Gespräch zu erwartende Aufforderung.

48 Siehe Fn. 11.

49 Vom 30.8.2007 in der Fassung vom 28.6.2024, chinesisch-deutsch abgedruckt in: ZChinR 2025, S. 256 ff.

50 Vom 29.6.2002 in der Fassung vom 10.6.2021, chinesischer Text abrufbar unter <lawinfochina.com> [北大法律英文网]/<pkulaw.cn> [北大法宝], Indexnummer [法宝引证码] CLI.1.5015195.

第六章　法律责任

第六十一条　网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可罚以处五万元以上十万元以下款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

6. Kapitel: Rechtliche Haftung

§ 61 [Sanktionen bei Verstoß gegen die §§ 23 und 27 (Netzwerkbetreiber), Sanktionen bei Verstoß gegen die §§ 35, 36, 38 und 40 (Betreiber wesentlicher Netzwerkinfrastruktur); Abs. 1 und Abs. 2 vgl. § 59 Abs. 1 und Abs. 2 a. F., Abs. 3 neu eingefügt] Erfüllen Netzwerkbetreiber die in den §§ 23 und 27 dieses Gesetzes festgelegten Pflichten zum Schutz der Netzwerksicherheit nicht, ordnen die betreffenden zuständigen Abteilungen eine Korrektur an, verwarnen [diese] und können eine Geldstrafe in Höhe von 10.000 bis 50.000 Yuan verhängen; wird die Korrektur verweigert oder führt [das Verhalten] zu Konsequenzen, wie etwa der Gefährdung der Netzwerksicherheit, wird eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt, gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt.

Erfüllen Betreiber wesentlicher Informationsinfrastruktur nicht die in den §§ 35, 36, 38 und 40 dieses Gesetzes festgelegten Pflichten zum Schutz der Netzwerksicherheit, ordnen die betreffenden zuständigen Abteilungen eine Korrektur an, verwarnen [diese] und können eine Geldstrafe in Höhe von 50.000 bis 100.000 Yuan verhängen. Wird die Korrektur verweigert oder führt das Verhalten zu Konsequenzen wie etwa der Gefährdung der Netzwerksicherheit, wird eine Geldstrafe in Höhe von 100.000 bis 1.000.000 Yuan verhängt; gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt.

Führen die in den beiden vorangehenden Absätzen beschriebenen Verhaltensweisen zu schwerwiegenden Konsequenzen der Gefährdung der Netzwerksicherheit wie etwa dem massenhaften Datenleck oder dem teilweisen Funktionsverlust wesentlicher Informationsinfrastruktur, wird von den betreffenden zuständigen Abteilungen eine Geldstrafe in Höhe von 500.000 bis 2.000.000 Yuan verhängt; gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 50.000 bis 200.000 Yuan verhängt. Führen sie zu besonders schwerwiegenden Konsequenzen der Gefährdung der Netzwerksicherheit wie etwa dem Verlust der Hauptfunktion wesentlicher Informationsinfrastruktur, wird eine Geldstrafe in Höhe von 2.000.000 bis 10.000.000 Yuan verhängt; gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 200.000 bis 1.000.000 Yuan verhängt.

第六十二条 违反本法第二十四条第一款、第二款和第五十条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

§ 62 [Sanktionen bei Verstoß gegen die §§ 24 und 50 (Anbieter von Netzwerkprodukten und -diensten); Abs. 1 und Abs. 2 vgl. § 60 a. F.; Abs. 3 neu eingefügt] Wird gegen die Bestimmungen der §§ 24 Abs. 1 und 2 oder § 50 Abs. 1 dieses Gesetzes verstoßen, so wird von den betreffenden zuständigen Abteilungen bei Vorliegen einer der nachfolgenden Verhaltensweisen eine Korrektur angeordnet und verwarnt; wird die Korrektur verweigert oder führt [das Verhalten] zu Konsequenzen, wie etwa der Gefährdung der Netzwerksicherheit, wird eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt, gegenüber direkt verantwortlichen zuständigen Mitarbeitern wird eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt:

（一）设置恶意程序的

1. Es wird Malware installiert;

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

2. es werden bezüglich der an ihren[51] Produkten oder -diensten bestehenden Risiken wie Sicherheitsmängeln oder -lücken nicht sofort Hilfsmaßnahmen ergriffen oder nicht den Bestimmungen gemäß unverzüglich die Nutzer benachrichtigt und [es wird nicht] den betreffenden zuständigen Abteilungen Bericht erstattet;

（三）擅自终止为其产品、服务提供安全维护的。

3. es wird eigenmächtig der für ihre Produkte oder Dienste zur Verfügung gestellte Sicherheitsschutz eingestellt.

有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

Bei Vorliegen der im vorangehenden Absatz genannten ersten oder zweiten Verhaltensweise, die zu den in § 61 Abs. 3 dieses Gesetzes bestimmten Konsequenzen führt, erfolgt die Sanktion gemäß den Bestimmungen jenes Absatzes.

第六十三条 违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。

§ 63 [Sanktionen bei Verstoß gegen § 25; neu eingefügt] Werden unter Verstoß gegen die Bestimmung des § 25 dieses Gesetzes wesentliche Netzwerkausstattung oder spezielle Netzwerksicherheitsprodukte verkauft oder zur Verfügung gestellt, die keiner Sicherheitsbestätigung oder Sicherheitsevaluierung unterzogen wurden oder die die Sicherheitsbestätigung nicht bestanden haben oder deren Sicherheitsevaluierung nicht den Anforderungen entspricht, so ordnen die betreffenden zuständigen Abteilungen an, den Verkauf oder die Zurverfügungstellung einzustellen, und sprechen eine Verwarnung aus; illegale Einkünfte werden beschlagnahmt. Liegen keine illegalen Einkünfte vor oder betragen die illegalen Einkünfte weniger als 100.000 Yuan, wird eine Geldstrafe in Höhe von 20.000 bis 100.000 Yuan verhängt; betragen die illegalen Einkünfte 100.000 Yuan oder mehr, wird eine Geldstrafe in Höhe des einfachen bis fünffachen Betrags der illegalen Einkünfte verhängt. Sind die Umstände schwerwiegend, kann zudem die vorübergehende Einstellung der relevanten Geschäftstätigkeit, die Betriebsstilllegung zur Korrektur, die Annullierung relevanter betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden. Enthalten Gesetze oder Verwaltungsrechtsnormen anderweitige Bestimmungen, so gelten diese Bestimmungen.

51 Bezug genommen wird auf die Anbieter von Netzwerkprodukten und -diensten, vgl. § 24.

第六十四条 网络运营者违反本法第二十六条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

§ 64 [Sanktionen bei Verstoß gegen § 26 (Netzwerkbetreiber); vgl. § 61 a. F.] Wenn Netzwerkbetreiber unter Verstoß gegen die Bestimmungen des § 26 Abs. 1 dieses Gesetzes von Kunden nicht die Zurverfügungstellung von Informationen über deren wahre Identität verlangen oder Kunden, die diese Informationen über ihre wahre Identität nicht zur Verfügung stellen, die betreffenden Dienste anbieten, ordnen die betreffenden zuständigen Abteilungen eine Korrektur an und verwarnen [sie]; wird die Korrektur verweigert oder liegen erschwerende Umstände vor, wird eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt und es kann zudem die vorübergehende Einstellung der relevanten Geschäftstätigkeit, die Betriebsstilllegung zur Korrektur, die Abschaltung von Internetseiten oder Anwendungen[52], die Annullierung relevanter betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden [und] gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt werden.

第六十五条 违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

§ 65 [Sanktionen bei Verstoß gegen § 28; Abs. 1 vgl. § 62 a. F., Abs. 2 neu eingefügt] Wird bei Aktivitäten wie der Durchführung von Bestätigungen, Prüfungen [oder] Risikobewertungen der Netzwerksicherheit oder der Veröffentlichung[53] von Netzwerksicherheitsinformationen wie etwa zu Systemanfälligkeiten, Computerviren, Netzwerkangriffen [oder] dem Eindringen ins Netzwerk gegen die Bestimmung des § 28 dieses Gesetzes verstoßen, wird von den betreffenden zuständigen Abteilungen eine Korrektur angeordnet, eine Verwarnung ausgesprochen und es kann eine Geldstrafe in Höhe von 10.000 Yuan bis 100.000 Yuan verhängt werden; wird die Korrektur verweigert oder liegen erschwerende Umstände vor, wird eine Geldstrafe in Höhe von 100.000 bis 1.000.000 Yuan verhängt und es kann zudem die vorübergehende Einstellung der relevanten Geschäftstätigkeit, die Betriebsstilllegung zur Korrektur, die Abschaltung von Internetseiten oder Anwendungen[54], die Annullierung relevanter betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden [und] gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt werden.

有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

Liegt ein im vorangehenden Absatz beschriebenes Verhalten vor und führt dieses zu den in § 61 Abs. 3 dieses Gesetzes bestimmten Konsequenzen, erfolgt die Sanktion gemäß den Bestimmungen jenes Absatzes.

52 Gemeint sind Apps.

53 Siehe Fn. 21.

54 Siehe Fn. 52

第六十六条 违反本法第二十九条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款.

§ 66 [Sanktionen bei Verstoß gegen § 29; vgl. § 63 a. F.] Werden unter Verstoß gegen § 29 dieses Gesetzes Aktivitäten ausgeführt, die die Netzwerksicherheit gefährden, oder werden Programme oder Werkzeuge zur Verfügung gestellt, die speziell zur Ausführung von die Netzwerksicherheit gefährdenden Aktivitäten genutzt werden, oder wird die Netzwerksicherheit gefährdende Hilfe wie etwa technologische Unterstützung, Inumlaufbringen von Werbung oder [Hilfe] bei der Abrechnung von Zahlungen zur Verfügung gestellt und hierdurch noch kein Straftatbestand erfüllt, werden illegale Einkünfte von den Behörden für öffentliche Sicherheit beschlagnahmt, ein Arrest von bis zu fünf Tagen verhängt [und] es kann eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt werden; sind die Umstände verhältnismäßig schwerwiegend, wird der Arrest für fünf bis 15 Tage verhängt und es kann eine Geldstrafe in Höhe von 100.000 bis 1.000.000 Yuan verhängt werden.

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚

Liegt bei einem Unternehmen[55] ein im voranstehenden Absatz beschriebenes Verhalten vor, so werden illegale Einkünfte von den Behörden für öffentliche Sicherheit beschlagnahmt, eine Geldstrafe in Höhe von 100.000 bis 1.000.000 Yuan verhängt und gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern eine Sanktion nach dem voranstehenden Absatz verhängt.

违反本法第二十九条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

Mitarbeiter, die gegen die Bestimmung des § 29 dieses Gesetzes verstoßen [und] eine Sanktion der öffentlichen Sicherheitsverwaltung erhalten haben, dürfen für fünf Jahre[56] keine Aufgaben der Netzwerksicherheitsverwaltung oder eine Schlüsselposition bei einem Netzwerkanbieter ausführen; wird gegen Mitarbeiter eine strafrechtliche Sanktion verhängt, dürfen [diese] lebenslänglich keine Aufgaben der Netzwerksicherheitsverwaltung oder Schlüsselpositionen bei einem Netzwerkanbieter ausführen.

第六十七条 关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

§ 67 [Sanktionen bei Verstoß gegen § 37 (Betreiber wesentlicher Informationsinfrastruktur); vgl. § 65 a. F.] Nutzen Betreiber wesentlicher Informationsinfrastruktur unter Verstoß gegen die Bestimmung des § 37 dieses Gesetzes Netzwerkprodukte oder -dienste, welche die Sicherheitstests nicht durchlaufen haben oder die Sicherheitstests nicht bestanden haben, wird von den betreffenden zuständigen Abteilungen eine fristgerechte Korrektur oder die Einstellung der Nutzung sowie die Beseitigung der Auswirkungen auf die staatliche Sicherheit angeordnet [und] eine Geldstrafe in Höhe des einfachen bis zehnfachen Anschaffungspreises[57] verhängt; gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt.

55 Wörtlich: „[Arbeits-]Einheit“.

56 Wörtlich: „innerhalb von 5 Jahren“.

57 Gemeint ist wohl das für die fraglichen Netzwerkprodukte oder -dienste gezahlte Entgelt.

第六十七条 违反本法第四十八条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚

§ 68 [Sanktionen bei Verstoß gegen § 48; vgl. § 67 a. F.] Werden unter Verstoß gegen die Bestimmung des § 48 dieses Gesetzes Internetseiten oder Gruppenkommunikationen errichtet, die dazu genutzt werden, rechtswidrige kriminelle Aktivitäten vorzunehmen, oder wird das Netzwerk dazu genutzt, Informationen zur Vornahme rechtswidriger krimineller Aktivitäten zu veröffentlichen, [und] wurde hierdurch noch kein Straftatbestand erfüllt, wird von den Behörden für öffentliche Sicherheit ein Arrest von bis zu fünf Tagen verhängt [und] es kann eine Geldstrafe in Höhe von 10.000 bis 100.000 verhängt werden; sind die Umstände verhältnismäßig schwerwiegend, wird der Arrest für fünf bis 15 Tage verhängt und es kann zudem eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt werden. Internetseiten oder Gruppenkommunikationen, die zur Vornahme rechtswidriger krimineller Aktivitäten genutzt wurden, werden geschlossen.

Liegt bei einem Unternehmen[58] ein im voranstehenden Absatz beschriebenes Verhalten vor, so wird von den Behörden für öffentliche Sicherheit eine Geldstrafe in Höhe von 100.000 bis 500.000 Yuan verhängt und gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Sanktion nach dem voranstehenden Absatz verhängt.

第六十九条 网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

§ 69 [Sanktionen bei Verstoß gegen §§ 49, 50 oder § 52; vgl. §§ 68, 69 Abs. 1 a. F., Abs. 2 neu eingefügt, Abs. 3 vgl. § 68 Abs. 2 a. F.] Verstoßen Netzwerkbetreiber gegen die Bestimmung des § 49 dieses Gesetzes, indem sie die Übertragung von Informationen, deren Veröffentlichung oderÜbertragung in Gesetzen oder Verwaltungsrechtsnormen verboten ist, nicht stoppen, keine Maßnahmen zur Handhabung wie etwa die Beseitigung [der Informationen] ergreifen [oder] keine betreffenden Aufzeichnungen speichern oder keine Meldung an die betreffenden zuständigen Abteilungen erstatten, oder verstoßen sie gegen die Bestimmung des § 52 dieses Gesetzes, indem sie nach Aufforderung der betreffenden Abteilungen die Übertragung von Informationen, deren Veröffentlichung oder Übertragung in Gesetzen oder Verwaltungsrechtsnormen verboten ist, nicht stoppen oder keine Maßnahmen wie etwa die Beseitigung ergreifen oder keine betreffenden Aufzeichnungen speichern, ordnen die betreffenden zuständigen Abteilungen eine Korrektur an, sprechen eine Verwarnung aus und geben eine öffentliche Mitteilung heraus; es kann eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt werden. Wird die Korrektur verweigert oder liegen erschwerende Umstände vor, wird eine Geldstrafe in Höhe von 500.000 bis 2.000.000 Yuan verhängt, und es kann die vorübergehende Einstellung der relevanten Geschäftstätigkeit, die Betriebsstilllegung zur Korrektur, die Abschaltung von Internetseiten oder Anwendungen[59], die Annullierung relevanter betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden; gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 50.000 bis 200.000 Yuan verhängt.

58 Gewählt ist hier der Ausdruck „[Arbeits-]Einheit“.

59 Siehe Fn. 52.

有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

Führen die im vorangehenden Absatz beschriebenen Verhaltensweisen zu besonders schwerwiegenden Auswirkungen oder besonders schwerwiegenden Konsequenzen, verhängen die betreffenden zuständigen Abteilungen eine Geldstrafe in Höhe von 2.000.000 bis 10.000.000 Yuan, ordnen die vorübergehende Einstellung der relevanten Geschäftstätigkeit, die Betriebsstilllegung zur Korrektur, die Abschaltung von Internetseiten oder Anwendungen[60], die Annullierung relevanter betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis an; gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern wird eine Geldstrafe in Höhe von 200.000 bis 1.000.000 Yuan verhängt.

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。

Erfüllen Anbieter von Diensten zur Sendung elektronischer Nachrichten und Anbieter von Diensten zum Herunterladen von Software unter Verstoß gegen die Bestimmung des § 50 dieses Gesetzes Sicherheitsverwaltungspflichten nicht, wird eine Sanktion nach den beiden voranstehenden Absätzen verhängt.

第七十条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

§ 70 [Sanktionen bei bestimmten Verhaltensweisen (Netzwerkbetreiber); vgl. § 69 a. F.] Gegenüber Netzwerkbetreibern, die gegen Bestimmungen dieses Gesetzes verstoßen, wird von den betreffenden zuständigen Abteilungen bei Vorliegen einer der nachfolgenden Verhaltensweisen eine Korrektur angeordnet; wird die Korrektur verweigert oder liegen erschwerende Umstände vor, wird eine Geldstrafe in Höhe von 50.000 bis 500.000 Yuan verhängt [und] gegenüber direkt verantwortlichen zuständigen Mitarbeitern und anderen direkt verantwortlichen Mitarbeitern eine Geldstrafe in Höhe von 10.000 bis 100.000 Yuan verhängt:

（一）绝、阻碍有关部门依法实施的监督检查的

1. Die gesetzmäßig vorgenommene Aufsicht und Untersuchung durch die betreffenden Abteilungen wird abgelehnt oder behindert;

（二）拒不向公安机关、国家安全机关提供技术支持和协助的

2. es wird abgelehnt, den Behörden für öffentliche Sicherheit oder staatlichen Sicherheitsbehörden technische Unterstützung und Hilfe zu leisten.

第七十一条 有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：

§ 71 [Weitere Verstöße und deren Sanktionierung; Nr. 1 vgl. § 70 a. F., Nr. 2 vgl. § 64 Abs. 1 a. F., Nr. 3 vgl. § 66 a. F., Abs. 2 vgl. § 64 Abs. 2 a. F.] Liegt eine der nachfolgenden Verhaltensweisen vor, erfolgt die Behandlung und Sanktionierung nach den betreffenden Bestimmungen der einschlägigen Gesetze und Verwaltungsrechtsnormen:

（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；

1. bei Veröffentlichung oder Übertragung von Informationen, deren Verbreitung oder Übertragung nach § 13 Abs. 2 dieses Gesetzes sowie anderer Gesetze oder Verwaltungsrechtsnormen verboten ist;

（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；

2. bei Verletzung der Rechte an persönlichen Informationen durch Verstoß gegen die Bestimmungen des § 24 Abs. 3 sowie der §§ 43 bis 45 dieses Gesetzes;

60 Siehe Fn. 52.

（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

3. bei Verstoß gegen die Bestimmung des § 39 dieses Gesetzes, indem Betreiber wesentlicher Informationsinfrastruktur persönliche Informationen und wichtige Daten im Ausland speichern oder persönliche Informationen und wichtige Daten im Ausland zur Verfügung stellen.

违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

Werden unter Verstoß gegen die Bestimmung des § 46 dieses Gesetzes persönliche Informationen gestohlen oder auf andere illegale Weise erlangt, illegal verkauft oder illegal Dritten zur Verfügung gestellt und ist damit noch kein Straftatbestand erfüllt, erfolgt die Sanktionierung durch die Behörden für öffentliche Sicherheit nach den betreffenden Bestimmungen der einschlägigen Gesetze und Verwaltungsrechtsnormen.

第七十二条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

§ 72 [Aufzeichnung von Verstößen in Unterlagen zur Kreditwürdigkeit und öffentliche Bekanntmachung; = § 65 a. F.] Liegt nach den Bestimmungen dieses Gesetzes ein rechtswidriges Verhalten vor, wird [dies] gemäß den betreffenden Bestimmungen in Gesetzen [oder] Verwaltungsrechtsnormen in Kreditwürdigkeitsregistern aufgezeichnet und öffentlich gemacht.

第七十三条 违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。

§ 73 [Milderung oder Unterlassung der Sanktion; neu eingefügt] Verstößt eine Person gegen die Bestimmungen dieses Gesetzes, liegen jedoch Umstände vor, die nach dem „Gesetz der Volksrepublik China über Verwaltungsstrafen" eine mildere Sanktion, eine Herabsetzung der Sanktion oder den Verzicht auf eine Sanktion rechtfertigen, so wird gemäß diesen Bestimmungen eine mildere Sanktion verhängt, die Sanktion herabgesetzt oder auf eine Sanktion verzichtet.

第七十四条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

§ 74 [Sanktionen bei Bezug zu Regierungsangelegenheiten; = § 72 a. F.] Erfüllen die Betreiber von Netzwerken bezüglich dienstlicher Angelegenheiten staatlicher Behörden nicht ihre Pflichten zum Schutz der Netzwerksicherheit, ordnen die übergeordneten Behörden oder die betreffende Behörde eine Korrektur an; gegen direkt verantwortliche zuständige Mitarbeiter und andere direkt verantwortliche Mitarbeiter werden gemäß dem Recht disziplinarische Maßnahmen verhängt.

第七十五条 网信部门和有关部门违反本法第三十二条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

§ 75 [Sanktionen bei Verstoß gegen § 32 (Abteilungen für Netzwerke und Informationen), Amtsmissbrauch; vgl. § 73 a. F.] Verstoßen Abteilungen für Netzwerke und Informationen oder betreffende Abteilungen gegen die Bestimmungen aus § 32 dieses Gesetzes und nutzen die in Erfüllung ihrer Amtspflichten zum Schutz der Netzwerksicherheit erlangten Informationen zu anderen Zwecken, [so] werden gegen direkt verantwortliche zuständige Mitarbeiter und andere direkt verantwortliche Mitarbeiter gemäß dem Recht disziplinarische Maßnahmen verhängt.

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

Kommen Mitarbeiter der Abteilungen für Netzwerke und Informationen oder betreffender Abteilungen ihren Amtspflichten nicht nach oder missbrauchen sie ihr Amt oder missbrauchen sie ihre Position zum persönlichen Nutzen [und] wird hierdurch noch kein Straftatbestand erfüllt, [so] werden gemäß dem Recht disziplinarische Maßnahmen verhängt.

第七十六条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十七条 境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

§ 76 [Zivile Haftung, Sicherheitsverwaltungssanktionen und strafrechtliche Haftung; = § 74 a. F.] Wer gegen die Bestimmungen dieses Gesetzes verstößt [und] eine Schädigung eines Dritten herbeiführt, trägt dem Recht gemäß die zivile Haftung.

Wird gegen die Bestimmungen dieses Gesetzes verstoßen [und] konstituiert dieses Verhalten einen Verstoß gegen die öffentliche Sicherheitsverwaltung, werden dem Recht gemäß Sicherheitsverwaltungssanktionen verhängt; konstituiert [dieses Verhalten] einen Straftatbestand, wird gemäß dem Recht die strafrechtliche Haftung verfolgt.

§ 77 [Sanktionen bei Aktivitäten ausländischer Einrichtungen, Organisationen oder Privatpersonen; vgl. § 75 a. F.] Gefährden Aktivitäten ausländischer Einrichtungen, Organisationen oder Privatpersonen die wesentliche Netzwerksicherheit der Volksrepublik China, wird gemäß dem Recht die rechtliche Haftung verfolgt; werden schwerwiegende Folgen herbeigeführt, können die Abteilung des Staatsrates für öffentliche Sicherheit und betreffende Abteilungen zudem entscheiden, Vermögen dieser Einrichtungen, Organisationen oder Privatpersonen einzufrieren oder andere nötige Sanktionsmaßnahmen zu ergreifen.

第七章 附则

7. Kapitel: Ergänzende Bestimmungen

第七十八条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

§ 78 [Begriffsbestimmungen; = § 76 a. F.] Die in diesem Gesetz genutzten, nachfolgend genannten Begriffe bedeuten:

1. Netzwerk bezeichnet ein von Computern oder anderen Informationsterminals und relevanter Ausrüstung gebildetes System, in dem Informationen gemäß konkreter Bestimmungen und Verfahren gesammelt, gespeichert, übertragen, ausgetauscht und gehandhabt werden.

2. Netzwerksicherheit bezeichnet das Verhindern von Angriffen auf das Netzwerk, Eindringen, Störung [oder] Zerstörung und illegale Nutzung sowie Unglücksfälle durch Ergreifen der nötigen Maßnahmen, [sodass das Netzwerk] in einen stabilen und verlässlichen Betriebszustand versetzt wird [und] die Fähigkeit der Netzwerkdaten zu Vollständigkeit, Geheimhaltung und Nutzbarkeit gewährleistet.

3. Netzwerkbetreiber bezeichnet die Eigentümer von Netzwerken, [Netzwerk-]Verwalter und Anbieter von Netzwerkdiensten.

4. Netzwerkdaten bezeichnet alle Arten von elektronischen Daten, die mittels eines Netzwerks gesammelt, gespeichert, übertragen, gehandhabt oder erstellt werden.

5. Persönliche Informationen bezeichnet alle Arten von Informationen, die elektronisch oder auf andere Weise aufgezeichnet werden [und] einzeln oder in Verbindung mit anderen Informationen die Identität einer Person unterscheiden können, einschließlich aber nicht begrenzt auf [Informationen] wie den Namen der natürlichen Person, das Geburtsdatum, die Personalausweisnummer, biometrische Unterscheidungsinformationen, die Adresse [oder] die Telefonnummer.

第七十九条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第八十条 军事网络的安全保护，由中央军事委员会另行规定。

第八十一条 本法自 2017 年 6 月 1 日起施行。

§ 79 [Anwendbarkeit anderer Normen; = § 77 a. F.] Beim Schutz der Betriebssicherheit von Netzwerken zur Speicherung oder Handhabung von Informationen über Staatsgeheimnisse müssen abgesehen von den Bestimmungen dieses Gesetzes auch die Bestimmungen der Gesetze und Verwaltungsrechtsnormen zur Geheimhaltung befolgt werden.

§ 80 [Sicherheitsschutz militärischer Netzwerke; = § 78 a. F.] Sicherheitsschutz für militärische Netzwerke wird separat von der Zentralen Militärkommission bestimmt.

§ 81 [Inkrafttreten; = § 79 a. F.] Dieses Gesetz wird vom 1.6.2017 an durchgeführt.

Übersetzung[61], Anmerkungen und Paragrafenüberschriften in eckigen Klammern von Peter Leibküchler, Düsseldorf

61 Die Übersetzung beruht auf der deutschen Übersetzung dieses Gesetzes in der Fassung vom 7.11.2016 (Fn. 2).