Verarbeiterpflichten im System chinesischer Netzwerk- und Datensicherheit

Jack J. Zipke *

* Der Autor ist Student der Rechtswissenschaften an der Martin-Luther-Universität Halle-Wittenberg und dort studentische Hilfskraft am Lehrstuhl für öffentliches Recht von Prof. Dr. Kluth. Von Februar bis März 2025 absolvierte er in Nanjing ein Praktikum am Deutsch-Chinesischen Institut für Rechtswissenschaften, in dessen Rahmen dieser Aufsatz entstanden ist. Der Autor dankt Rainer Burkardt und Ondřej Zapletal, beide Rechtsanwälte bei Burkardt & Partner in Shanghai, für ihre wertvollen Anmerkungen aus der Praxis, die Eingang in diesen Aufsatz gefunden haben.

ZChinR 2025: S. 119–132
DOI: 10.71163/zchinr.2025.119-132

Abstract

Am 30. August 2024 hat der chinesische Staatsrat die „Verordnung zur Verwaltung der Netzwerkdatensicherheit" verabschiedet, die seit dem 1. Januar 2025 zur Anwendung kommt. Damit werden Regulierungen zur Sicherheit im digitalen Raum zusammengeführt und ergänzt. Dieser Aufsatz gibt zunächst einen Überblick über die zentralen Rechtsquellen mit Bezug zu Netzwerken und Daten sowie deren gemeinsame Konzeption. Anschließend werden grundlegende Begriffe erläutert. Darauf aufbauend werden die Pflichten für Verarbeiter von Daten in Abhängigkeit zu den verarbeiteten Daten und den Umständen der Verarbeitung erläutert. Zudem wird auf die Durchsetzung der dargestellten Pflichten eingegangen. Der Aufsatz gibt eine systematische Hilfestellung an die Hand, die vor allem das Auffinden der relevanten Normen und der in ihnen niedergeschriebenen Pflichten erleichtern soll.

Processor Obligations in the Chinese Network and Data Security System *— On 30 August 2024, the Chinese State Council passed the "Regulation on the Administration of Network Data Security", which has been in effect since 1 January 2025. This regulation consolidates and supplements existing rules on digital security. This article first provides an overview of the key legal sources related to networks and data, along with their shared conceptual foundation. It then explains fundamental terms and outlines the obligations for data processors based on the type of data processed and the processing circumstances. Additionally, it addresses the enforcement of these obligations. The article offers a systematic guide designed to facilitate the identification of relevant legal provisions and the obligations contained within them.*

I. Einführung

Mit der chinesischen Rechtsetzung zu Netzwerken und Daten unternimmt die Volksrepublik nunmehr seit 2016 den Versuch, Herrin über die Sicherheit im digitalen Raum zu werden. In den letzten Jahren hat sich eine Vielzahl an Bestimmungen angehäuft, die Akteure im digitalen Raum mit einer noch größeren Zahl an Normbefehlen konfrontiert. Dabei kann schnell der Überblick darüber verloren gehen, welche Verpflichtungen einen etwa beim Umgang mit Netzwerken und Daten treffen. Dieser Aufsatz soll Struktur in diese Verpflichtungen bringen.

Dazu wird zunächst auf die relevanten Rechtsquellen (dazu II.) und die daraus ableitbaren allgemeinen Konzepte der Regulierung von Netzwerken und Daten (dazu III.) eingegangen. Anschließend werden zentrale Begriffe erläutert (dazu IV.) und erklärt, welche verschiedenen Pflichtenträger die Rechtsquellen adressieren (dazu V.) Darauf aufbauend werden die Pflichten im Einzelnen, kategorisiert nach ihren Voraussetzungen, systematisch dargestellt (dazu VI. bis VIII.). Abschließend wird noch kurz auf die Durchsetzung der Pflichten eingegangen (dazu IX.).

II. Rechtsquellen

Die älteste der hier zu betrachtenden Rechtsquellen ist das „Netzwerksicherheitsgesetz der Volksrepublik China"[1] aus 2016 (im Folgenden: „NetzwSichG"). Dieses reguliert gemäß § 2 NetzwSichG umfassend Aufbau, Betrieb, Schutz und Nutzung von Netzwerken[2]. Es folgten 2021 erst das „Datensicherheitsgesetz der Volksrepublik China"[3] (im Folgenden: „DatenSichG") und dann das „Gesetz der Volksrepublik China zum Schutz persönlicher Daten"[4] (im Folgenden: „PersDatenSchG"). Ersteres erfasst jede Verarbeitung von Daten[5], letzteres nur persönliche Daten natürlicher Personen. 2024 folgte die eingangs erwähnte „Verordnung zur Verwaltung der Netzwerkdatensicherheit"[6] (im Folgenden: „NetzwDatenSichVO"), die auf den Schutz von Netzwerkdaten abzielt.

III. Konzepte der chinesischen Netzwerk- und Datenregulierung

Um das chinesische Konzept zur Regulierung von Netzwerken und Daten zu verstehen, muss zunächst ein Blick auf das chinesische Verständnis von Sicherheit gerichtet werden. Dieses

1 中华人民共和国网络安全法 vom 7.11.2026, chinesisch-deutsch in: ZChinR 2018, S. 113 ff. (dort als „Cybersicherheitsgesetz" übersetzt).

2 Zum Begriff der Netzwerke siehe unten unter IV.1.

3 中华人民共和国数据安全法 vom 10.6.2021, chinesisch-deutsch in diesem Heft, S. 162 ff.

4 中华人民共和国个人信息保护法 vom 20.8.2021, chinesisch-deutsch in: ZChinR 2021, S. 286 ff.; dieses Gesetz sorgte auch für Kompatiblität des Datenschutzes im vierten Buch des ZGB (中华人民共和国民法典 vom 28.5.2020, chinesisch-deutsch in: ZChinR 2020, S. 207 ff.) und dem DatenSichG.

5 Zum Begriff der Datenverarbeitung siehe unten unter VII.1.

6 网络数据安全管理条例 vom 30.8.2024, chinesisch-deutsch in diesem Heft, S. 175 ff.

geht über die Wahrung der öffentlichen Sicherheit und Ordnung im engeren Sinne hinaus. 2014 formulierte Xi Jinping das „umfassende Konzept staatlicher Sicherheit“[7] auf der ersten Sitzung der zentralen Kommission für staatliche Sicherheit der Kommunistischen Partei Chinas[8]. Demnach müssen für eine umfassende Sicherheit eine Vielzahl an Themen betrachtet werden. Hierzu zählen neben politischer, wirtschaftlicher und finanzieller Sicherheit auch die technologische und die Netzwerksicherheit.[9] Der Umsetzung dieses Systems dient die Rechtsetzung zur Netzwerk- und Datensicherheit (§ 4 DatenSichG, § 3 NetzwDatenSichVO).

Auf dieser Grundlage wird gemäß § 21 NetzwSichG ein „mehrstufiges Schutzsystem der Netzwerksicherheit“ (网络安全等级保护制度) aufgebaut. Dieses wird durch § 31 Abs. 1 NetzwSichG dahingehend ausgestaltet, dass schwerpunktmäßig wichtige Branchen und Bereiche geschützt werden sollen, was vor allem wesentliche Infrastruktur betrifft. Dieses System bildet gemäß § 27 Abs. 1 Satz 2 DatenSichG auch die Basis für den Schutz von Daten bei deren Verarbeitung unter der Nutzung von Netzwerken.

Die Daten selbst unterliegen wiederum gemäß § 21 Abs. 1 DatenSichG und § 5 NetzwDatenSchG einem „klassifizierten und eingestuften Schutz“ (分类分级保护), wonach Daten nach ihrer Wichtigkeit für die sozioökonomische Entwicklung und ihrem Gefahrenpotenzial für die staatliche Sicherheit einzustufen sind. Dieses Einstufungssystem erfolgt über Kataloge, die durch alle Regionen (地区)[10] und Abteilungen (部门)[11] zu erstellen sind (§ 21 Abs. 3 DatenSichG, § 29 Abs. 1 NetzwDatenSichVO).

IV. Begriffe

Nach dieser Konzeption bilden Netzwerke (dazu 1.) und Daten (dazu 2.) zwei zentralen Schutzgüter der staatlichen Sicherheit. Diese Begriffe werden im Folgenden erläutert. Es soll außerdem auf einige zentrale Behörden und Abteilungen eingegangen werden (dazu 3.).

1. Netzwerke

Als Netzwerke (网络) definiert § 76 Nr. 1 NetzwSichG Systeme, die aus Computern oder anderen Informationsterminals bestehen und Informationen nach konkreten Bestimmungen und Verfahren sammeln, speichern, übertragen, austauschen und handhaben. Damit ist vordergründig, aber nicht ausschließlich, das Internet (互联网) gemeint.

Als besondere Teilnetzwerke lassen sich Netzwerkplattformen ansehen. Deren Anbieter werden daher besonders reguliert und unter IV. näher beleuchtet.

2. Daten

Der regulatorische Fokus liegt klar auf Daten (数据). Diese definiert § 3 Abs. 1 DatenSichG als „jegliche Aufzeichnungen von Informationen in elektronischer oder anderer Form“. Informationen als Möglichkeit abstrakter Wahrnehmbarkeit von Wissen bilden damit die Grundlage und werden durch Daten als deren Trägerinnen zu gesetzlichen Schutzobjekten.[12]

Nach dem Konzept der Klassifizierung und Einstufung von Daten lassen sich diese näher differenzieren:

Es gibt wichtige Daten (重要数据), die von § 62 Nr. 4 NetzwDatenSichVO abstrakt damit beschrieben werden, dass sie mit Bezug zu bestimmten Gebieten (领域)[13], Gruppen (群体)[14] oder Regionen (区域)[15] oder aufgrund ihrer Genauigkeit oder ihres Umfangs eine Gefahr für die staatliche Sicherheit, den Wirtschaftsbetrieb, die gesellschaftliche Stabilität oder die öffentliche Gesundheit und Sicherheit darstellen können, wenn sie verfälscht, zerstört, weitergegeben, illegal erhalten oder genutzt werden. Diese recht vage Umschreibung muss durch alle Regionen und Abteilungen ausgefüllt werden, indem sie gemäß § 21 Abs. 3 DatenSichG und § 29 Abs. 1 NetzwDatenSichVO Kataloge wichtiger Daten erstellen müssen.[16]

7 Chinesisch: „总体国家安全观“.

8 Chinesisch: „中央国家安全委员会“.

9 *Kerry Liu*, The economics of China's Holistic View of National Security: A preliminary assessment, in: Economic Affairs, Vol. 44 (2024), S. 218 ff., abrufbar unter: <https://doi.org/10.1111/ecaf.12646>.

10 Regionen meint hierbei wohl Verwaltungsgebiete, etwa in Form von Landkreisen, Städten oder Stadtteilen. Damit dürfte etwas Ähnliches wie die Verbandszuständigkeit von Gebietskörperschaften im deutschen Recht gemeint sein.

11 Abteilungen bezeichnen hier wohl generelle Stellen öffentlicher Verwaltung.

12 *Vincent Winkler*, Rechte an Daten im Zivilrecht, Tübingen 2021, S. 25.

13 Hiermit sind wohl abstrakte Bereiche oder Themengebiete gemeint, wie etwa der Wissenschaft, Politik oder Religion.

14 Hiermit sind wohl Gruppen von Menschen gemeint, wie etwa Berufsstände, soziale Schichten oder ethnische Minderheiten.

15 Hiermit sind wohl konkrete und abgegrenzte geografische Gebiete gemeint, etwa in Form von Wirtschaftszonen oder Funktionsbereichen.

16 Hierzu wurde am 15.3.2024 der Standard „Informationssicherheitstechnik: Regeln für die Klassifizierung und Einstufung von Daten“ (数据安全技术数据分类分级规则) (GB/T 43697-2024) erlassen, abrufbar unter www.tc260.org.cn (<https://perma.cc/44JD-WB8D>).

Eine besondere Untergruppe wichtiger Daten stellen Kerndaten (核心数据) dar, welche gemäß § 21 Abs. 2 DatenSichG Bezug zur staatlichen Sicherheit, zu der Lebensader der Volkswirtschaft oder wichtigen öffentlichen Interessen haben. Da die untersuchten Rechtsquellen dazu nur die Aussage treffen, dass sie verstärkt und streng verwaltet werden müssen, bleiben sie im Weiteren außer Betracht.

Persönliche Daten (个人信息) wiederum bezeichnen gemäß § 4 Abs. 2 PersDatenSchG und § 76 Nr. 5 NetzwSichG aufgezeichnete Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, also allein oder in Verbindung mit anderen Informationen die Identität einer Person unterscheiden können. Der chinesische Begriff steht wörtlich übersetzt zwar für „Informationen von Einzelpersonen", allerdings stellt auch die gesetzliche Definition auf die Aufzeichnung der Informationen ab, womit alle Merkmale des Datenbegriffs vorliegen. Somit kann trotz abweichender chinesischer Terminologie der Begriff „persönliche Daten" verwendet werden.[17] Beispiele für persönliche Daten sind etwa Namen, E-Mail-Adressen oder Telefonnummern.

Eine Untergruppe persönlicher Daten sind sensible persönliche Daten (敏感个人信息). Diese umfassen gemäß § 28 Abs. 1 PersDatenSchG solche, die im Falle der Weitergabe oder illegalen Verwendung typischerweise die Würde, die Sicherheit oder das Vermögen der betroffenen Person verletzen.[18] Immer sensibel gemäß dieser Norm sind auch persönliche Daten von Minderjährigen, die jünger als 14 Jahre sind.

Die letzte zu nennende Kategorie sind Netzwerkdaten (网络数据). Diese werden gemäß § 62 Nr. 1 NetzwDatenSichVO dadurch charakterisiert, dass sie durch Netzwerke gesammelt oder verarbeitet werden. Dadurch sind sie, anders als die zuvor genannten Daten, ausschließlich in elektronischer Form aufgezeichnet.

17 Vgl. *Vincent Winkler*, a. a. O. (Fn. 12), S. 23.

18 Als Beispiele sensibler persönlicher Daten nennt die Vorschrift Informationen über biometrische Identifizierung, Religion oder Glaube, eine bestimmte Identität, medizinische Behandlung, Gesundheit, Finanzkonten, Aufenthaltsort und Ortswechsel. Dazu gehören beispielsweise auch Personalausweisnummern, Bankkontoinformationen, Wohnadressen oder Gesundheitsdaten. Genauere Anleitungen zur Identifizierung persönlicher Daten bietet auch der Standard „Informationssicherheitstechnik: Normung der Sicherheit persönlicher Daten" (信息安全技术 个人信息安全规范) (GB/T 35273-2020) vom 6.3.2020, auf Englisch abrufbar unter www.tc260.org.cn (<https://perma.cc/6Z4V-QNKD>).

3. Behörden und Abteilungen

Die untersuchten Quellen enthalten eine Vielzahl an Behörden und Abteilungen, deren Bezeichnungen aus den Normen selbst heraus aber keine konkrete Zuordnung der Zuständigkeiten enthalten.

So wird an vielen Stellen etwa schlicht auf „zuständige Behörden" (相关部门) oder „betreffende zuständige Abteilungen" (有关主管部门) verwiesen. Der Normgeber verwendet solche oder ähnliche Formulierungen deswegen, weil im Zeitpunkt der Normierung meist nicht feststeht, welche konkreten Abteilungen oder Behörden für eine Aufgabe zuständig sein sollen. Dies wird, wenn überhaupt, erst später festgelegt.

Etwas konkreter wird der Normgeber immerhin dann, wenn er auf „staatliche Abteilungen für Netzwerke und Informationen" (国家网信部门) verweist. Diese umfassen staatliche Abteilungen sämtlicher Stufen, insbesondere die „Cyberspace Administration of China" (CAC, 中华人民共和国国家互联网信息办公室), die identisch mit dem sogenannten „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) ist.[19] Diese Abteilungen sind gemäß § 47 Abs. 1 NetzwDatenSichVO vor allem für Koordinationsaufgaben zuständig.

Gemäß § 47 Abs. 2 NetzwDatenSichVO sind im Übrigen wohl vor allem die staatlichen Sicherheitsbehörden (国家安全机关) und die Behörden für öffentliche Sicherheit (公安机关) die zuständigen betreffenden Abteilungen. Diese sind Verwaltungsbehörden, die beide für die Ermittlung rechtswidrigen Verhaltens zuständig sind. Dabei sind erstere vor allem für die Wahrung der Staatssicherheit zuständig, etwa durch die Verhinderung von Straftaten oder anderer schwerwiegender Aktivitäten. Letztere sind zuständig für weniger schwerwiegende kriminelle Aktivitäten.

V. Pflichtenträger

Die Pflichten zum Schutz der genannten Rechtsgüter liegen, abgesehen von den staatlichen Institutionen, bei den Datenverarbeitern (dazu 1.). Eine Sonderform derer sind Netzwerkbetreiber (dazu 2.). Daneben gibt es weitere Personengruppen, denen durch die Rechtsnormen Pflichten auferlegt werden (dazu 3.). Einige Pflichten gelten zudem für jeden und jede (diese werden im Kontext allgemeiner Pflichten unten unter VI. dargestellt).

19 Siehe die betreffende Anmerkung zum Cybersicherheitsgesetz (Fn. 1) in der Übersetzung von *Peter Leibküchler*, in: ZChinR 2018, S. 115 (dort: Fn. 8).

1. Datenverarbeiter

Datenverarbeiter (数据处理者) sind Einzelpersonen oder Organisationen, die Daten verarbeiten. Verarbeitung ist der zentrale Prozess, der durch die verschiedenen Normen adressiert und dessen Sicherheit gewährleistet werden soll. Sie umfasst sämtliche Aktivitäten im Hinblick auf Daten (§ 3 Abs. 2 DatenSichG), persönliche Daten (§ 4 Abs. 2 PersDatenSchG) oder Netzwerkdaten (§ 62 Nr. 2 NetzwDatenSichVO), insbesondere sammeln, speichern, nutzen, bearbeiten, übertragen, bereitstellen, offenlegen oder löschen. Dabei treffen Verarbeiter selbstständig die Entscheidung über die Verarbeitungszwecke und -mittel (§ 73 Nr. 1 PersDatenSchG, § 62 Nr. 3 NetzwDatenSichVO). Nicht erfasst wird gemäß § 72 Abs. 1 PersDatenSchG und § 63 Abs. 2 NetzwDatenSichVO die Verarbeitung durch Einzelpersonen wegen persönlichen oder familiären Angelegenheiten („Haushaltsprivileg“).

In Abhängigkeit von den verarbeiteten Daten gibt es damit Datenverarbeiter, Verarbeiter wichtiger Daten, Verarbeiter persönlicher Daten und Verarbeiter von Netzwerkdaten. Besonderheiten bestehen zudem für Verarbeiter, die sich außerhalb des Gebiets Chinas befinden und Daten von in China befindlichen Personen verarbeiten. Auf die Pflichten dieser einzelnen Verarbeiter wird unten unter VII. eingegangen.

2. Netzwerkbetreiber

Weitere Pflichtenträger sind Netzwerkbetreiber (网络运营者), die von § 76 Nr. 3 NetzwSichG als Eigentümer und Verwalter von Netzwerken und als Anbieter von Netzwerkdiensten definiert werden. Diese werden wohl zumeist auch in irgendeiner Art und Weise Netzwerkdaten verarbeiten, weshalb sie als spezielle Art von Verarbeitern von Netzwerkdaten und gegebenenfalls Verarbeitern persönlicher Daten angesehen werden können. Eine weitere Unterform dieser Pflichtenträger bilden Betreiber wesentlicher Informationsinfrastruktur (关键信息基础设施运营者).

Ähnliches gilt für Netzwerkplattformendiensteanbieter (网络平台服务提供者), die durch die NetzwDatenSichVO als Pflichtenträger benannt, aber nicht definiert werden. Sofern man Netzwerkplattformendienste ihrerseits als Netzwerkdienste ansieht, handelt es sich bei deren Anbietern somit um eine Unterform von Netzwerkbetreibern.

3. Sonstige Pflichtenträger

Neben Verarbeitern nennt etwa § 22 NetzwSichG Anbieter von Netzwerkprodukten und -diensten (网络产品、服务的提供者). § 33 DatenSichG erwähnt zudem Vermittler von Datenhandel.[20] Auch diese sind Träger von Pflichten[21], werden aber ebenfalls nicht definiert.

VI. Allgemeine Pflichten für jeden und jede

Im Hinblick auf die Netzwerksicherheit wird durch § 12 Abs. 2 NetzwSichG eine allgemeine Pflicht zur Rechtstreue und ein Verbot der Gefährdung der Netzwerksicherheit aufgestellt. Netzwerke dürfen darüber hinaus nicht für eine Reihe gefährlicher Aktivitäten verwendet werden. Eine nähere Ausgestaltung erfährt dies durch § 27 NetzwSichG, nach dem etwa das Eindringen in oder das Stören von fremden Netzwerken oder der Diebstahl von Netzwerkdaten verboten wird. Ebenso verboten ist das Bereitstellen von Programmen oder Werkzeugen, die speziell für das Eindringen, Stören oder Stehlen verwendet werden. Bei Kenntnis solcher Aktivitäten ist auch das Hilfe leisten verboten. Mit § 8 NetzwDatenSichVO werden diese Verbote auch auf die illegale Verarbeitung von Netzwerkdaten erweitert. Gemäß § 39 NetzwDatenSichVO gilt zusätzlich ein Bereitstellungsverbot für Programme und Werkzeuge, die der Umgehung oder Zerstörung technischer Maßnahmen dienen. Zudem darf keine Hilfe bei der Umgehung oder Zerstörung geleistet werden. Aufgrund der systematischen Stellung im 5. Kapitel zur Sicherheit der Verwaltung grenzüberschreitender Netzwerkdaten dürften mit diesen Programmen und Werkzeugen wohl vor allem VPN-Dienste gemeint sein.

Weiter wird die Nutzung von Netzwerken durch § 46 NetzwSichG reguliert. Danach trägt jeder Verantwortung für sein Verhalten der Netzwerknutzung: Niemand darf Netzwerke für die Vornahme illegaler Aktivitäten errichten oder darf auf diesen Informationen bezüglich illegaler Aktivitäten verbreiten. Gemäß § 48 Abs. 1 NetzwSichG ist es verboten, Software zu senden oder bereitzustellen, die Malware installiert oder Informationen enthält, deren Veröffentlichung oder Übertragung verboten sind.

Nach § 44 NetzwSichG ist es schließlich verboten, persönliche Daten rechtswidrig zu erhalten oder zur Verfügung zu stellen.

20 Diese werden im Gesetz als Organe bezeichnet, die in der Vermittlung von Datenhandel tätig sind (从事数据交易中介服务的机构).

21 Zu den Pflichten siehe unten unter VIII.

VII. Die Pflichten von Verarbeitern im Einzelnen

Im Folgenden werden die Pflichten der Verarbeiter einzeln dargestellt. Zunächst wird auf allgemeine Pflichten beim Verarbeiten von Daten eingegangen (dazu 1.). Danach folgen die Pflichten der spezifischen Arten von Verarbeitern: Verarbeiter von Netzwerkdaten (dazu 2.), Netzwerkbetreiber (dazu 3.), Netzwerkplattformendiensteanbieter (dazu 4.), Verarbeiter wichtiger Daten (dazu 5.) und Verarbeiter persönlicher Daten (dazu 6.). Abschließend werden besondere Pflichten im Zusammenhang mit grenzüberschreitenden Sachverhalten wiedergegeben (dazu 7.).

1. Allgemeine Pflichten beim Verarbeiten von Daten

Allgemeine Pflichten, die bei der Verarbeitung von Daten beachtet werden müssen, ergeben sich aus den §§ 27, 29 und 32 DatenSichG. Gemäß § 27 Abs. 1 DatenSichG muss etwa ein starkes System der Datensicherheit errichtet werden, Bildung zu Datensicherheit erfolgen und die Datensicherheit muss durch notwendige Maßnahmen gewährleistet werden. Gemäß § 29 DatenSichG müssen die Risikoüberwachung verstärkt und bei Risiken sofort Abhilfemaßnahmen ergriffen werden. Verdichten sich diese Risiken zu Datensicherheitsvorfällen, müssen unverzüglich die Nutzer und die betreffende zuständige Abteilung informiert werden. Nach § 32 DatenSichG müssen Daten durch legale und gerechtfertigte Mittel gesammelt werden und es ist verboten, sie rechtswidrig zu erhalten.

Im Hinblick auf schlichte Daten gibt es damit wenige Vorgaben für die Verarbeitung. Dies liegt vor allem daran, dass das DatenSichG – wie oben unter II. erläutert – primär die Errichtung staatlicher Strukturen reguliert.

2. Pflichten von Verarbeitern von Netzwerkdaten

Neben den allgemeinen Pflichten hält die NetzwDatenSichVO für Verarbeiter von Netzwerkdaten weitere Pflichten bereit. Gemäß § 9 NetzwDatenSichVO sind sie zum Schutz von Netzwerkdaten verpflichtet und müssen dazu Verwaltungssysteme aufbauen und technische Schutzmaßnahmen ergreifen, um Verfälschung, Zerstörung, Weitergabe und illegale Nutzung von Daten zu verhindern.

Insbesondere muss auch für Netzwerkdatensicherheitsvorfälle vorgesorgt werden. Dazu müssen die Verarbeiter von Netzwerkdaten gemäß § 11 Abs. 1 NetzwDatenSichVO einen Notfallplan aufstellen und diesen im Falle von Netzwerkdatensicherheitsvorfällen ausführen, Maßnahmen zur Eindämmung und Beseitigung der Gefahren ergreifen und die betreffenden zuständigen Abteilungen informieren. Abs. 2 Satz 1 dieser Vorschrift normiert weitergehend detaillierte Anforderungen an die Information für Betroffene, wenn deren Rechte oder Interessen gefährdet sind. Werden Spuren zu rechtswidrigen kriminellen Hintergründen gefunden, muss nach dessen Abs. 2 Satz 2 auch den dort genannten Behörden Anzeige erstattet und mit diesen kooperiert werden.

Weitere Pflichten ergeben sich aus besonderen Modalitäten der Verarbeitung:

Wenn die Verarbeitung die staatliche Sicherheit beeinflusst oder beeinflussen kann, muss gemäß § 13 NetzwDatenSichVO ein staatlicher Sicherheitstest durchgeführt werden. Die zu Sicherheitstests ergehenden Entscheidungen sind gemäß § 24 Abs. 2 DatenSichG endgültig.

Erweiterte Pflichten ergeben sich auch beim Einsatz automatisierter Werkzeuge und künstlicher Intelligenz. Für automatisierte Werkzeuge muss gemäß § 18 NetzwDatenSichVO eine Bewertung ihres Einflusses auf Netzwerkdienste vorgenommen werden. Durch sie darf nicht illegal in fremde Netzwerke eingedrungen oder der Betrieb von Netzwerkdiensten gestört werden. Werden Dienste generativer künstlicher Intelligenz angeboten, muss sich die Sicherheit der Verwaltung gemäß § 19 NetzwDatenSichVO auch auf die Trainingsdaten und deren Verarbeitung erstrecken und es müssen wirksame Maßnahmen zur Risikovorbeugung ergriffen werden.

Besonders wird schließlich die Übertragung von Netzwerkdaten reguliert. Falls dies etwa aufgrund von Vereinigung, Spaltung oder Konkurs notwendig ist, ist die Empfängerseite gemäß § 14 NetzwDatenSichVO zum Schutz der Netzwerkdatensicherheit verpflichtet. Werden einem anderen Verarbeiter von Netzwerkdaten Netzwerkdaten bereitgestellt oder wird dieser mit deren Verarbeitung beauftragt und handelt es sich bei den Daten um wichtige oder persönliche Daten, müssen gemäß § 12 Abs. 1 NetzwDatenSichVO die Zwecke, Mittel und Bereiche der Verarbeitung und Pflichten zum Schutz der Netzwerkdatensicherheit vereinbart werden. Nach dieser Vorschrift muss der Auftraggeber auch die Erfüllung der Pflichten durch die Empfängerseite überwachen und die Aufzeichnung über die betroffenen Daten müssen drei Jahre aufbewahrt werden. Nach dessen Abs. 2 muss die Empfängerseite ihre Pflichten entsprechend erfüllen. Abs. 3

dieser Norm regelt den Fall der gemeinsamen Verarbeitung und ordnet für diesen Fall an, dass die Verarbeiter von Netzwerkdaten ihre jeweiligen Rechte und Pflichten vereinbaren müssen.

3. Pflichten von Netzwerkbetreibern

Als Sonderform von Verarbeitern von Netzwerkdaten treffen Netzwerkbetreiber zunächst auch die oben unter 2. dargestellten und zusätzlich die folgenden Pflichten.

Zunächst verpflichtet § 21 NetzwSichG sie auf Grundlage des mehrstufigen Schutzsystems der Netzwerksicherheit allgemein zum Schutz von Netzwerken vor Störung, Zerstörung und unbefugten Zugriffen. Es müssen etwa ein internes Sicherheitsverwaltungssystem festgelegt und technische Maßnahmen ergriffen werden, insbesondere zur Klassifizierung von Daten, Sicherung wichtiger Daten und Verschlüsselung. Außerdem muss nach dieser Vorschrift ein Verantwortlicher für Netzwerksicherheit bestimmt werden.

Einige weitere Pflichten sollen hier nur kurz wiedergegeben werden: Gemäß § 25 NetzwSichG gelten die gleichen Pflichten zur Aufstellung von Notfallplänen und die bei Netzwerksicherheitsvorfällen wie für Verarbeiter von Netzwerkdaten gemäß § 11 NetzwDatenSichVO. Gemäß § 28 NetzwSichG sind Netzwerkbetreiber zur Unterstützung der Behörden für öffentliche Sicherheit und der staatlichen Sicherheitsbehörden bei der rechtmäßigen Wahrung der staatlichen Sicherheit und der Ermittlung von kriminellen Aktivitäten verpflichtet.

Für Betreiber wesentlicher Informationsinfrastruktur ergeben sich zusätzliche Pflichten aus den §§ 34–38 NetzwSichG. Diese müssen gemäß § 34 NetzwSichG strenge Sicherheitsschutzpflichten erfüllen, wie etwa die Einsetzung eines speziellen Sicherheitsverwaltungsorgans, die Schulung ihres Personals, die Durchführung von Notfallsicherungen und das Festlegen eines Notfallplans für Störfälle. Gemäß § 35 NetzwSichG müssen bei potenziell gefährlichen Netzwerkprodukten und -diensten Sicherheitstests und gemäß § 38 NetzwSichG eine jährliche Sicherheitsüberprüfung durchgeführt werden. Gemäß § 36 NetzwSichG müssen die Betreiber wesentlicher Informationsinfrastruktur beim Erwerb von Netzwerkprodukten oder -diensten eine Sicherheits- und Verschwiegenheitsvereinbarung unterzeichnen. Werden persönliche oder wichtige Daten gesammelt, müssen diese gemäß § 37 Satz 1 NetzwSichG grundsätzlich im chinesischen Inland gespeichert werden.

Weitere Pflichten sind im 4. Kapitel des NetzwSichG im Hinblick auf Netzwerkinformationen normiert. Zunächst müssen gesammelte Nutzerinformationen gemäß § 40 NetzwSichG streng geheim gehalten und ein starkes Schutzsystem aufgebaut werden. Gemäß § 47 NetzwSichG müssen Netzwerkbetreiber vor allem die durch Nutzer veröffentlichten Informationen überwachen. Sollten sie dabei Informationen entdecken, deren Veröffentlichung oder Übertragung verboten ist, müssen sie die Übertragung stoppen, die Ausbreitung verhindern, die betreffenden Aufzeichnungen speichern und der betreffenden zuständigen Abteilung Bericht erstatten. Das Gleiche gilt gemäß § 48 Abs. 2 NetzwSichG auch im Hinblick auf Dienste zur Sendung elektronischer Nachrichten und zum Herunterladen von Software, die Malware installieren oder verbotene Informationen enthalten. Damit wird das nutzerseitige Verbot gemäß § 48 Abs. 1 NetzwSichG umgesetzt (siehe hierzu oben VI.).

Gemäß § 49 Abs. 1 NetzwSichG müssen Netzwerkbetreiber ein Beschwerde- und Anzeigesystem aufbauen, darüber informieren und Beschwerden und Anzeigen annehmen und bearbeiten. Gemäß Abs. 2 dieser Norm müssen sie zudem mit den Abteilungen für Netzwerke und Informationen bei ihrer Aufsicht und Untersuchung zusammenarbeiten.

Die §§ 41–43 NetzwSichG stellen einige weitere Pflichten im Hinblick auf persönliche Daten auf. Diese gehen allerdings völlig in den Pflichten als Pflichten von Verarbeitern persönlicher Daten auf.

Weitere Pflichten können sich gemäß § 50 NetzwSichG aus Anordnungen der Abteilungen für Netzwerke und Informationen ergeben.

4. Pflichten von Netzwerkplattformendiensteanbietern

Für Netzwerkplattformendiensteanbieter gelten als Sonderform der Netzwerkbetreiber neben allen bisher beschriebenen Pflichten zusätzlich die folgenden.

Die NetzwDatenSichVO sieht zunächst eine Reihe von Pflichten der Netzwerkplattformendiensteanbieter im Hinblick auf die ihre Plattformen betretenden Drittanbieter von Waren und Diensten vor. So müssen sie nach § 40 Abs. 1 NetzwDatenSichVO etwa durch Plattformregeln, Vertrag oder in anderer Form für die Drittanbieter deutlich Pflichten zum Schutz der Netzwerkdatensicherheit benennen und die Drittanbieter zur Verstärkung der Sicherheit anhalten. Gemäß Abs. 2 dieser Norm erstreckt

sich die Pflicht zum Aufstellen solcher Pflichten auch auf Produzenten von Smart-Terminals mit vorinstallierten Anwendungsprogrammen[22] und anderen Anlagen. Bieten Netzwerkplattformendiensteanbieter Dienste zur Verteilung von Anwendungsprogrammen an, müssen sie gemäß § 41 NetzwDatenSichVO zusätzlich Überprüfungsregeln errichten und bei Anwendungsprogrammen, die nicht im Einklang mit den rechtlichen oder sonstigen staatlichen Vorgaben stehen, entsprechende Maßnahmen ergreifen. Bei den hier regulierten Diensten handelt es sich wohl vor allem um App-Stores. Verstoßen die Drittanbieter bei der Datenverarbeitung gegen Gesetze, Verwaltungsrechtsnormen, Plattformregeln oder Verträge und schädigen sie dadurch die Nutzer, haften die Drittanbieter gemäß § 40 Abs. 3 NetzwDatenSichVO gemeinsam mit den Netzwerkplattformendiensteanbietern und den ihnen gleichgestellten Produzenten.

Nutzen Netzwerkplattformendiensteanbieter automatisierte Push-Benachrichtigungen, müssen sie den Nutzern gemäß § 42 NetzwDatenSichVO einfach verständliche und bequem durchführbare Optionen und Funktionen zum Ablehnen personalisierter Empfehlungen, von Push-Benachrichtigungen und zum Löschen personalisierter „Nutzertags" (用户标签)[23] anbieten.

Zusätzliche Pflichten ergeben sich bei großen Netzwerkplattformen. Solche liegen gemäß § 62 Nr. 8 NetzwDatenSichVO vor, wenn eine der folgenden Bedingungen erfüllt ist:

- Sie haben 50 Millionen registrierte Nutzer;
- sie haben monatlich zehn Millionen aktive Nutzer;
- sie betreiben „komplizierte Geschäftstypen" (业务类型复杂) oder
- sie betreiben Geschäftstypen, die einen wichtigen Einfluss auf die staatliche Sicherheit, den Wirtschaftsbetrieb oder die Lebenshaltung der Bevölkerung haben.

Die Anbieter solcher großen Netzwerkplattformen müssen gemäß § 44 NetzwDatenSichVO jährlich einen Bericht zur gesellschaftlichen Verantwortung zum Schutz persönlicher Daten abgeben, dessen Mindestinhalt in der Norm auch vorgegeben ist. Durch § 46 NetzwDatenSichVO wird ihnen außerdem verboten, Netzwerkdaten, Algorithmen und Plattformregeln für bestimmte Aktivitäten zu benutzen. Beispielsweise dürfen Nutzerdaten nicht durch Irreführung, Täuschung oder Drohung verarbeitet werden; Nutzern darf nicht grundlos die Nutzung oder der Zugriff auf ihre Daten verwehrt werden und sie dürfen nicht unvernünftig ungleich behandelt werden oder in ihren Rechten und Interessen geschädigt werden. Diese Norm kann aber nur klarstellenden Charakter haben. Es ist schwer vorstellbar, dass die genannten Handlungen nicht für alle Netzwerkplattformendiensteanbieter verboten sein sollen.

5. Pflichten von Verarbeitern wichtiger Daten

Verarbeitung wichtiger Daten liegt dann vor, wenn Verarbeiter von Netzwerkdaten wichtige Daten verarbeiten. Für Verarbeiter von Netzwerkdaten ist daher zunächst wichtig, dass sie die von ihnen verarbeiteten Daten gemäß § 29 Abs. 2 NetzwDatenSichVO als wichtige Daten identifizieren und dann den betreffenden Regionen und Abteilungen melden müssen. Für die Identifikation ermutigt der Staat gemäß § 29 Abs. 3 NetzwDatenSichVO dazu, Label (标签)[24] oder andere Technologien zu verwenden. Wenn die Daten daraufhin als wichtige Daten bestätigt werden, müssen die Verarbeiter von Netzwerkdaten die zusätzlichen folgenden Pflichten als Verarbeiter wichtiger Daten erfüllen.

Verarbeiter wichtiger Daten müssen zunächst gemäß § 27 Abs. 2 DatenSichG einen Verantwortlichen und ein Verwaltungsorgan für Netzwerkdatensicherheit benennen. Die konkreten Pflichten des Verwaltungsorgans ergeben sich aus § 30 Abs. 1 NetzwDatenSichVO. Dazu gehört etwa auch die Festlegung und Umsetzung von Notfallplänen für Netzwerkdatensicherheitsvorfälle, das Annehmen und Bearbeiten von Beschwerden und Anzeigen und die Durchführung von Risikobewertungen. Der Verantwortliche für Datensicherheit muss gemäß § 30 Abs. 2 NetzwDatenSichVO über spezielle Kenntnisse verfügen. Er ist nach dieser Norm kraft Amtes befugt, den betreffenden zuständigen Abteilungen

22 Chinesisch: „预装应用程序的智能终端". Damit sind laut einer Erläuterung der KI „DeepSeek" Geräte gemeint, die mit vorinstallierter Software verkauft bzw. ausgeliefert werden. Darunter fallen demnach Geräte wie Smartphones, Tablets, Smart-TVs oder Smartwatches.

23 Dabei handelt es sich laut einer Erläuterung der KI „DeepSeek" um Kennzeichnungen oder Kategorien, mit denen Benutzerprofile organisiert werden. Diese Tags bilden etwa demografische Informationen oder Informationen zu Verhaltensweisen, Interessen oder dem verwendeten Gerät ab. Anders als Cookies, die clientseitig auf dem Gerät des Nutzers gespeichert werden, sind Nutzer-Tags serverseitig gespeichert.

24 Gemeint sein dürfte hiermit, dass Kategorien von Daten mit Kennzeichnungen versehen werden. Dadurch können diese gesammelt den betreffenden Regionen und Abteilungen gemeldet werden.

direkt Bericht über den Zustand der Netzwerkdatensicherheit zu erstatten. Gemeint ist damit wohl, dass er sich nicht zunächst an seinen Vorgesetzten zu wenden hat. Werden wichtige Daten besonderer Art oder besonderen Ausmaßes „beherrscht" (掌握)[25], muss gemäß § 30 Abs. 3 NetzwDatenSichVO bei dem Verantwortlichen für Netzwerkdatensicherheit und Angestellten auf Schlüsselpositionen eine Überprüfung des sicherheitsrelevanten Hintergrundes erfolgen. Ab welcher Art und welchem Ausmaß dies erforderlich ist, wird gemäß dieser Vorschrift von der betreffenden zuständigen Abteilung bestimmt.

Gemäß § 30 DatenSichG, § 33 Abs. 1 NetzwDatenSichVO muss eine jährliche Risikobewertung durchgeführt und der betreffenden zuständigen Abteilung auf Provinzebene oder einer höheren Ebene gemeldet werden. Abs. 2 dieser Norm gibt hierfür einen Mindestinhalt vor. Bei großen Netzwerkplattformendiensteanbietern erweitert Abs. 3 der Norm diesen Mindestinhalt.

Eine Risikobewertung muss gemäß § 31 Abs. 1 NetzwDatenSichVO auch durchgeführt werden, bevor wichtige Daten einem anderen bereitgestellt werden, dieser mit der Verarbeitung beauftragt wird oder wichtige Daten gemeinsam verarbeitet werden. Dabei gilt ein eigener schwerpunktmäßiger Inhalt für die Risikobewertung, der in Abs. 2 der Norm näher bestimmt wird. Diese Pflicht gilt nach § 31 Abs. 1 a. E. NetzwDatenSichVO nicht, wenn die Bereitstellung, Beauftragung oder gemeinsame Verarbeitung zur Erfüllung gesetzlicher Pflichten gehört.

Bei der Übertragung wichtiger Daten unter Umständen, die die Netzwerkdatensicherheit beeinflussen können, müssen gemäß § 32 NetzwDatenSichVO zusätzliche Maßnahmen ergriffen werden und der betreffenden zuständigen Abteilung auf Provinzebene oder einer höheren Ebene ein Handhabungskonzept und die Informationen der Empfängerseite mitgeteilt werden. Die Verordnung nennt dabei Umstände wie etwa Vereinigung, Spaltung, Auflösung oder Konkurs.

6. Pflichten von Verarbeitern persönlicher Daten

a) Grundlegende Pflichten

Das PersDatenSchG regelt einerseits die Voraussetzungen für die Erhebung und Verarbeitung persönlicher Daten. Die NetzwDatenSichVO stellt ergänzende Vorgaben auf und regelt auch die Pflichten, wenn eine rechtmäßige Erhebung nicht möglich ist. Verarbeiter persönlicher Daten unterliegen einem umfangreich ausgestalteten Pflichtenprogramm. Die Verarbeitung hat zunächst gemäß §§ 5–8 PersDatenSichG nach gewissen Grundsätzen zu erfolgen, wie etwa dem der Datenminimierung oder der Zweckbindung

Eine rechtmäßige Verarbeitung persönlicher Daten setzt voraus, dass eine der Voraussetzungen des § 13 PersDatenSchG vorliegt oder sie durch andere Bestimmungen erlaubt wird. Besondere Vorgaben gibt es dabei, wenn die Verarbeitung auf einer Einwilligung beruht. Gemäß § 14 Abs. 1 PersDatenSchG ist etwa erforderlich, dass die Einwilligung in vollständiger Kenntnis und freiwillig abgegeben wurde. Aus Abs. 2 dieser Vorschrift ergibt sich, dass sich die Einwilligung auch nur auf bestimmte Zwecke oder Mittel der Verarbeitung bezieht und dass bei deren Änderung eine erneute Einwilligung erforderlich ist. Durch § 22 NetzwDatenSichVO werden die Pflichten weiter ausgestaltet und konkrete Vorgaben zum Umgang mit der Einwilligung gemacht. Die Einwilligung kann gemäß § 15 Abs. 1 PersDatenSchG jederzeit widerrufen werden. Hierfür muss der Verarbeiter persönlicher Daten nach dieser Norm eine bequeme Möglichkeit anbieten. Wegen des Widerrufs darf gemäß § 16 PersDatenSchG die Leistung von Waren und Diensten nur eingestellt werden, wenn die Verarbeitung der persönlichen Daten dafür erforderlich ist. Die persönlichen Daten müssen gemäß § 19 PersDatenSchG einer möglichst kurzen Speicherfrist unterliegen.

Sofern eine rechtmäßige Datenerhebung nicht möglich ist, etwa weil automatisierte Sammeltechnologien verwendet werden, müssen die persönlichen Daten gemäß § 24 NetzwDatenSichVO grundsätzlich gelöscht oder anonymisiert werden. Ist dies technisch schwierig oder unzulässig, muss die Datenverarbeitung eingestellt werden, außer im Hinblick auf Sicherheits- und Schutzmaßnahmen.

Verarbeiter persönlicher Daten treffen gemäß § 17 PersDatenSchG eine Informationspflicht, die sie vor der Verarbeitung der Daten erfüllen müssen. Der in § 17 PersDatenSchG normierte Mindestinhalt dieser Information wird durch § 21 NetzwDatenSichVO näher konkretisiert. Von der Informationspflicht können sie gemäß § 18 PersDatenSchG befreit sein, wenn nach Gesetzen oder Verwaltungsrechtsnormen eine Geheimhaltungspflicht besteht oder dringende Umstände vorliegen. In letzterem Fall muss die Information nach dieser Norm unverzüglich nachgeholt werden.

Gemäß § 51 PersDatenSchG müssen Verarbeiter persönlicher Daten eine Reihe von Schutz-

25 Gemeint sein dürfte hiermit, dass Verarbeiter die Verfügungsgewalt über diese Daten haben.

maßnahmen zur Gewährleistung der Rechtskonformität und Datensicherheit ergreifen. Insbesondere werden in § 51 Nr. 5, 6 PersDatenSchG auch Notfallpläne für Sicherheitsvorfälle und regelmäßige Schulungen erwähnt. Ab einer von den Abteilungen für Netzwerke und Informationen bestimmten Menge verarbeiteter persönlicher Daten muss gemäß § 52 PersDatenSchG zudem ein Verantwortlicher für den Schutz persönlicher Daten bestimmt werden.[26] Im Hinblick auf den Schutz persönlicher Daten müssen Verarbeiter persönlicher Daten gemäß § 54 PersDatenSchG und Verarbeiter wichtiger Daten gemäß § 27 NetzwDatenSichVO periodische Compliance-Audits durchführen. Bestehen Gefahren der Weitergabe, Verfälschung oder des Verlustes persönlicher Daten, müssen gemäß § 57 Abs. 1 PersDatenSchG sofort Abhilfemaßnahmen ergriffen und die zuständigen Abteilungen und die betroffenen Personen informiert werden.

In den Fällen des § 55 PersDatenSchG muss im Vorfeld der Verarbeitung eine Folgenabschätzung mit dem durch § 56 PersDatenSchG vorgegebenen Mindestinhalt vorgenommen werden. Dies ist nach der nicht abschließenden Liste in § 55 PersDatenSchG erforderlich bei sensiblen persönlichen Daten, Mitteln automatisierter Entscheidungsfindung, Beauftragung mit der Verarbeitung, Bereitstellung oder Offenlegung und Bereitstellung an einen anderen außerhalb Chinas.

b) Pflichten unter besonderen Umständen

Für Fälle der Verarbeitung persönlicher Daten durch mehrere Verarbeiter persönlicher Daten bestehen zusätzliche Pflichten. Für die Bereitstellung persönlicher Daten an einen anderen Verarbeiter persönlicher Daten ist gemäß § 23 PersDatenSchG zunächst erforderlich, die betroffene Person zu informieren und eine separate Einwilligung einzuholen. Werden Daten gemeinsam verarbeitet,[27] müssen gemäß § 20 Abs. 1 PersDatenSchG die Rechte und Pflichten zwischen den Verarbeitern persönlicher Daten vereinbart werden. Sie tragen zudem gemäß § 20 Abs. 2 PersDatenSchG die gesamtschuldnerische Haftung für den Fall, dass die Rechte und Interessen an persönlichen Daten verletzt und eine Schädigung verursacht wird. Wird ein anderer mit der Verarbeitung beauftragt, müssen gemäß § 21 Abs. 1 PersDatenSchG neben den Rechten und Pflichten auch die Zwecke, Mittel, Fristen, Kategorien und Schutzmaßnahmen der Verarbeitung vereinbart werden und der Auftraggeber muss hierüber die Aufsicht führen. Wird der Vertrag aufgehoben oder ist er unwirksam, müssen die persönlichen Daten gemäß § 21 Abs. 2 Hs. 2 PersDatenSchG zurückgegeben oder gelöscht werden. Eine Unterbeauftragung ist ohne Einverständnis des Auftraggebers gemäß § 21 Abs. 3 PersDatenSchG unzulässig. Bei notwendiger Übertragung aufgrund etwa von Vereinigung oder Spaltung müssen gemäß § 22 PersDatenSchG die Betroffenen informiert werden und der Empfänger die Pflichten des ursprünglichen Verarbeiters weiter erfüllen.

Weitere Pflichten bestehen für besondere Arten der Verarbeitung. Solche Pflichten sind beispielsweise bei „automatisierter Entscheidungsfindung“ (自动化决策) normiert. Diese wird durch § 73 Nr. 2 PersDatenSchG als Verfahren definiert, bei dem Angelegenheiten betroffener Personen wie etwa Verhaltensgewohnheit, Hobbys oder Wirtschafts-, Gesundheits- und Kreditwürdigkeitsstatus automatisch analysiert, bewertet und eine Entscheidungsfindung durchgeführt wird. Werden Mittel einer solchen automatisierten Entscheidungsfindung verwendet, muss der Verarbeiter persönlicher Daten gemäß § 24 Abs. 1 PersDatenSchG die Transparenz, Gerechtigkeit und Unparteilichkeit gewährleisten. Kommt diese Entscheidungsfindung auch für Benachrichtigungen oder kommerzielles Marketing zum Einsatz, müssen gemäß Abs. 2 der Vorschrift Optionen zum Verweigern im Ganzen oder nur im Hinblick auf Personalisierung angeboten werden. Bei Entscheidungen, die schwerwiegende Auswirkungen auf Rechte und Interessen der Betroffenen haben können, haben diese gemäß Abs. 3 der Norm das Recht, Aufklärung zu verlangen und eine automatisierte Entscheidung zu verweigern.

Auf öffentlichen Plätzen dürfen Kameras gemäß § 26 PersDatenSchG nur zur Aufrechterhaltung der öffentlichen Sicherheit angebracht und die Aufnahmen nur dafür verwendet werden. Zusätzlich ist das Anbringen auffälliger Hinweisschilder erforderlich.

Eine Offenlegung persönlicher Daten ist gemäß § 25 PersDatenSchG nur mit einer separaten Einwilligung zulässig. Legen Personen persönliche Daten selbst offen oder wurden sie durch andere rechtmäßig offengelegt, dürfen sie gemäß § 27 PersDatenSchG grundsätzlich auch in angemessenem Umfang verarbeitet werden, außer die

26 Die „bestimmten Mengen“ sind in Art. 11.1 des Standards „Informationssicherheitstechnik: Normung der Sicherheit persönlicher Daten“ (GB/T 35273-2020) (Fn. 18) festgelegt.

27 Das Gesetz nennt als Tatbestandsvoraussetzung, dass mehrere Verarbeiter persönlicher Daten die Zwecke und Mittel der Verarbeitung gemeinsam entscheiden. Diese Voraussetzung wird durch § 62 Nr. 5 NetzwDatenSichVO als „gemeinsame Verarbeitung“ definiert.

betroffene Person verweigert die Verarbeitung. Bei schwerwiegenden Auswirkungen muss nach dieser Norm zunächst die Einwilligung eingeholt werden.

Sofern persönliche Daten von zehn Millionen oder mehr Personen als Netzwerkdaten verarbeitet werden, müssen gemäß § 28 NetzwDatenSichVO zudem die Pflichten der §§ 30 und 32 NetzwDatenSichVO erfüllt werden, also ein Verantwortlicher und ein Organ für Netzwerkdatensicherheit benannt und Maßnahmen zur Gewährleistung der Netzwerkdatensicherheit im Falle beeinflussender Umstände (wie etwa Vereinigung, Spaltung, Auflösung oder Konkurs des Verarbeiters) ergriffen werden. Werden „wesentliche Dienste" (重要服务) über Internetplattformen erbracht oder haben die Verarbeiter persönlicher Daten eine „riesige Anzahl an Nutzern" (用户数量巨大) oder komplizierte Geschäftstypen, müssen sie gemäß § 58 PersDatenSchG unter anderem ein Compliance-System errichten, unabhängige Organe mit externen Mitgliedern gründen, Plattformregeln festlegen, deren Inhalt in der Norm geregelt ist, Anbietern illegaler Inhalte ihre Plattform nicht mehr bereitstellen, einen Bericht zur Verantwortung zum Schutz persönlicher Daten bekannt machen und sich der sozialen Aufsicht unterstellen.

c) Pflichten im Umgang mit sensiblen persönlichen Daten

Besonderen Schutz erfahren sensible persönliche Daten.[28] Diese dürfen gemäß § 28 Abs. 2 PersDatenSchG nur für einen bestimmten Zweck, bei absoluter Notwendigkeit und unter strengen Schutzmaßnahmen verarbeitet werden. Gemäß § 29 PersDatenSchG ist eine separate Einwilligung des Betroffenen erforderlich. Die Verarbeiter persönlicher Daten müssen gemäß § 30 PersDatenSchG zusätzlich zu den Informationspflichten aus § 17 Abs. 1 PersDatenSchG über die Notwendigkeit der Verarbeitung informieren. Bei Minderjährigen, die jünger als 14 Jahre alt sind, muss gemäß § 31 PersDatenSchG eine Einwilligung des Vormundes (d. h. in der Regel der Eltern[29]) eingeholt werden und es müssen spezielle Regeln für die Verarbeitung festgelegt werden.

d) Umgang mit Betroffenenrechten

Betroffene haben gemäß §§ 44–49 PersDatenSchG eine Reihe von Rechten im Hinblick auf ihre persönlichen Daten, etwa auf Auskunft, Einsichtnahme, Übertragung oder Löschung. Diese Rechte korrespondieren mit Pflichten der Verarbeiter persönlicher Daten. Diese müssen zunächst gemäß § 50 Abs. 1 PersDatenSchG einen bequemen Mechanismus für die Ausübung der Betroffenenrechte einrichten. Lehnt ein Verarbeiter persönlicher Daten ab, die betreffenden Pflichten zu erfüllen, muss er dies nach jener Norm begründen. Durch § 23 NetzwDatenSichVO wird diese Pflicht dahingehend näher ausgestaltet, dass Verarbeiter von Netzwerkdaten die Forderungen, mit denen Betroffene ihre Rechte ausüben, unverzüglich annehmen und bearbeiten und Hilfe bei der Ausübung der Rechte bereitstellen müssen. Sie dürfen gemäß dieser Vorschrift keine unvernünftigen Voraussetzungen an die Ausübung der Rechte knüpfen. Grundsätzlich bestehen keine Voraussetzungen für die Rechte der Betroffenen. Dies gilt nicht bei der Löschung nach § 47 PersDatenSchG und der Übertragung nach § 45 Abs. 3 PersDatenSchG. Für die Löschung enthält § 47 Abs. 1 PersDatenSchG eine nicht abschließende Liste von Situationen, in denen der Betroffene die Löschung der Daten verlangen kann, soweit der Verarbeiter nicht seiner Pflicht nachkommt, die Daten von sich aus zu löschen. Im Fall der Übertragung ergeben sich die Voraussetzungen aus § 25 Abs. 1 NetzwDatenSichVO. Wird unvernünftig häufig die Übertragung gefordert, kann der Verarbeiter von Netzwerkdaten hierfür gemäß Abs. 2 der Norm Gebühren fordern.

7. Besondere Pflichten bei grenzüberschreitenden Sachverhalten

Aufgrund der besonderen Sicherheitsrelevanz werden Daten zusätzlich reguliert, wenn es zu einem Datenaustausch über die Landesgrenzen Chinas hinweg kommt.[30]

Die Bereitstellung persönlicher Daten ins Ausland ist gemäß § 38 Abs. 1 PersDatenSchG und § 35 Abs. 1 NetzwDatenSichVO nur zulässig, wenn eine der dort genannten Erlaubnisgründe vorliegt. Die „Bestimmungen zur Förderung und

28 Zur Definition sensibler persönlicher Daten siehe oben unter IV.2.

29 Siehe § 27 Abs. 1 Zivilgesetzbuch der Volksrepublik China (中华人民共和国民法典), chinesisch-deutsch in: ZChinR 2020, S. 207 ff.

30 Gemeint ist hier wie üblich China ohne Hongkong, Macao und Taiwan. Dies wird auch in der NetzwDatenSichVO deutlich durch die Formulierung „außerhalb des Gebiets [der VR China]" (境外). Siehe etwa § 35 NetzwDatenSichVO.

Normierung des grenzüberschreitenden Umlaufs von Daten“[31] enthalten weitere Erlaubnisgründe und regeln konkretere Anforderungen an die Erlaubnisgründe.[32] Gemäß § 39 PersDatenSchG muss der Verarbeiter persönlicher Daten außerdem eine separate Einwilligung der Betroffenen einholen.

Die Abteilungen für Netzwerke und Informationen können gemäß § 42 PersDatenSchG eine „schwarze Liste“ führen und die Bereitstellung an die darin aufgeführten Personen und Organisationen beschränken oder verbieten. Das ist nach dieser Vorschrift gedacht für diejenigen, die Rechte und Interessen chinesischer Bürger an persönlichen Daten verletzen.

Die Bereitstellung persönlicher Daten an ausländische Gerichte oder Institutionen darf gemäß § 41 Satz 2 PersDatenSchG nur nach Genehmigung der zuständigen Behörde erfolgen.

Betreiber wesentlicher Infrastruktur und Verarbeiter persönlicher Daten, die eine große Menge persönlicher Daten verarbeiten, müssen die persönlichen Daten gemäß § 40 Satz 1 PersDatenSchG grundsätzlich im Inland speichern. Ist die Bereitstellung in das Ausland „wirklich notwendig“ (确需), muss nach § 40 Satz 2 PersDatenSchG eine Sicherheitsbewertung[33] bestanden werden. Gemäß § 37 NetzwDatenSichVO ist es nun auch für die Bereitstellung wichtiger Daten ins Ausland erforderlich, dass eine Sicherheitsbewertung für ausgehende Daten bestanden wurde. Durch die genannten „Bestimmungen zur Förderung und Normierung des grenzüberschreitenden Umlaufs von Daten“ werden Ausnahmen für die Durchführung dieser Sicherheitsbewertungen normiert. Verarbeiter von Netzwerkdaten sind gemäß § 38 NetzwDatenSichVO an die in der Sicherheitsbewertung benannten Zwecke, Mittel, Bereiche und Arten der Verarbeitung gebunden.

Wenn ausländische Verarbeiter persönlicher Daten innerhalb Chinas persönliche Daten verarbeiten, müssen sie gemäß § 53 PersDatenSchG ein spezielles Organ errichten oder einen Repräsentanten bestimmen, das bzw. der die Angelegenheiten zum Schutz persönlicher Daten regeln muss. Den örtlichen Abteilungen für Netzwerke und Informationen müssen gemäß § 26 NetzwDatenSichVO gewisse Informationen zu dem Organ oder dem Repräsentanten gemeldet werden.

VIII. Pflichten von Produkte- und Diensteanbietern

Anbieter von Netzwerkprodukten oder -diensten müssen gemäß § 22 Abs. 1 Satz 1 NetzwSichG sicherstellen, dass die Netzwerkprodukte oder -dienste den „zwingenden Anforderungen relevanter staatlicher Standards“ (国家标准的强制性要求) genügen. Werden an diesen Risiken entdeckt, müssen nach § 22 Abs. 1 Satz 2 NetzwSichG Abhilfemaßnahmen ergriffen und die Nutzer und die betreffenden zuständigen Abteilungen informiert werden. Es muss außerdem gemäß § 22 Abs. 1 Satz 3 NetzwSichG ein dauerhafter Sicherheitsschutz bereitgestellt werden. Für Verarbeiter von Netzwerkdaten, die Netzwerkprodukte oder -dienste bereitstellen, wiederholt § 10 NetzwDatenSichVO diese Pflichten. Ergänzt wird in § 10 a. E. NetzwDatenSichVO, dass im Falle der Gefährdung der staatlichen Sicherheit oder öffentlicher Interessen den Abteilungen innerhalb von 24 Stunden Bericht erstattet werden muss.

Bestimmte Dienste, die vor allem mit Information und Kommunikation in Verbindung stehen, dürfen gemäß § 24 Abs. 1 NetzwSichG nur angeboten werden, wenn die wahre Identität des Kunden bestätigt wurde.

Werden die Waren und Dienste für die Allgemeinheit bereitgestellt, ergeben sich für die Verarbeiter von Netzwerkdaten aus § 20 NetzwDatenSichVO zusätzliche Pflichten hinsichtlich der öffentlichen Aufsicht (durch die Pflicht zur öffentlichen Bekanntmachung der Regeln für die Verarbeitung persönlicher Daten, deren Inhalt die Vorschrift normiert) und der Annahme und Bearbeitung von Beschwerden und Anzeigen. Wenn sie für Behörden, wesentliche Informationsinfrastruktur oder öffentliche Infrastruktur Dienste anbieten, sind sie gemäß § 16 NetzwDatenSichVO für jede Verarbeitung auf die Zustimmung des Auftraggebers angewiesen.

Wesentliche Netzwerkausstattung und spezielle Sicherheitsprodukte dürfen gemäß § 23 NetzwSichG erst nach einer Bestätigung der Sicherheitskonformität verkauft oder angeboten werden.

Schließlich muss bei Diensten des Datenhandels dessen Anbieter gemäß § 33 DatenSichG verlangen, dass der Bereitsteller die Quelle der

31 促进和规范数据跨境流动规定 vom 7.11.2026, chinesisch-deutsch in: ZChinR 2024, S. 159 ff.

32 Siehe hierzu ausführlich *Rainer Burkardt/Ondřej Zapletal*, CAC-Bestimmungen zur Förderung und Regulierung des grenzüberschreitenden Datenverkehrs – Echte Erleichterungen des strengen Datenschutzregimes für KMU in China?, in: ZChinR 2024, S. 128 ff. (128 ff.).

33 Siehe hierzu ausführlich *Rainer Burkardt/Ondřej Zapletal*, Sicherheitsbewertung für grenzüberschreitende Datentransfers aus China, in: ChinaContact 5/6 2022, abrufbar unter <https://www.bktlegal.com> (<https://perma.cc/A4KY-ANS7>).

Daten erklärt und dass Bereitsteller und Empfänger ihre Identitäten belegen. Die Aufzeichnungen hierüber müssen aufbewahrt werden.

IX. Durchsetzung der Pflichten

Ergänzend soll nun noch ein Blick darauf geworfen werden, welche Mittel die untersuchten Rechtsquellen zur Durchsetzung der vorgestellten Pflichten bereithalten. Zunächst wird auf Eingriffsbefugnisse eingegangen, die Abteilungen und Behörden zur Verfügung stehen (dazu 1.). Danach werden Sanktionen betrachtet, die bei Verstößen verhängt werden können (dazu 2.). Abschließend wird noch auf die Haftung nach anderen Gesetzen eingegangen (dazu 3.).

1. Eingriffsbefugnisse

Abteilungen für Netzwerke und Informationen oder betreffende Abteilungen müssen gemäß § 50 NetzwSichG bei der Verbreitung von verbotenen Informationen gegenüber Netzwerkbetreibern „Handhabungsmaßnahmen" (处置措施) anordnen. Insbesondere muss nach dieser Vorschrift ein Verbreitungsstopp angeordnet werden. Beim Eintritt von Netzwerksicherheitsstörfällen muss gemäß § 55 NetzwSichG von Netzwerkbetreibern verlangt werden, Maßnahmen zu ergreifen.

Im Falle von Sicherheitsrisiken im Hinblick auf Datensicherheit oder die Netzwerksicherheit oder treten Netzwerksicherheitsstörfälle ein, können zuständige Abteilungen gemäß § 56 NetzwSichG beziehungsweise § 44 DatenSichG zu „Gesprächen bitten" (约谈) und Maßnahmen zu Korrekturen oder der Beseitigung latenter Gefahren anordnen.

Im Hinblick auf den Schutz persönlicher Daten enthält § 63 Abs. 1 PersDatenSchG Eingriffsbefugnisse für zuständige Abteilungen. Nach dieser Vorschrift können sie betreffende Parteien um Auskunft ersuchen, in betreffende Verträge Einsicht nehmen und diese kopieren, Vor-Ort-Audits durchführen, um möglicherweise rechtswidrige Datenverarbeitung zu ermitteln und betreffende Anlagen und Gegenstände überprüfen. Gemäß § 64 Abs. 1 PersDatenSchG können bei größeren Risiken oder Sicherheitsvorfällen betreffend persönlicher Daten auch Befragungen durchgeführt und die Beauftragung eines Fachorgans mit der Durchführung von Compliance-Audits angeordnet werden.

Entsprechende Eingriffsbefugnisse enthält § 50 NetzwDatenSichVO im Hinblick auf die Sicherheit von Netzwerkdaten. Nach dieser Vorschrift, die im Hinblick auf die Befugnisse nicht abschließend ist, kann von Verarbeitern und ihrem Personal verlangt werden, eine Erklärung zu Angelegenheiten der Aufsicht und Untersuchung abzugeben oder Einsicht in Schriftstücke zu gewähren und diese zu kopieren, und es können Untersuchungen im Hinblick auf die Betriebssituation oder zu Anlagen und Gegenständen durchgeführt werden. Zusätzliche Befugnisse ergeben sich aus § 33 Abs. 4 NetzwDatenSichVO im Hinblick auf staatsgefährdende Verarbeitung wichtiger Daten und aus § 54 NetzwDatenSichVO im Hinblick auf staatsgefährdende Aktivitäten außerhalb Chinas.

2. Sanktionen

In Abhängigkeit von den jeweiligen Verstößen halten die Gesetze weitergehende Sanktionen bereit. Deren Inhalte werden hier nur zusammenfassend und verallgemeinernd wiedergegeben.[34]

Meistens werden bei Verstößen zunächst Korrekturen angeordnet, es wird verwarnt und gegebenenfalls werden illegale Einkünfte in Beschlag genommen. Darüber hinaus sind auch Geldstrafen möglich. Deren Verhängung liegt teilweise im Ermessen der betreffenden zuständigen Abteilungen, teilweise ist die Verhängung auch zwingend. Sie können sowohl den betreffenden Organisationen oder Einzelpersonen als auch „direkt verantwortlichem Personal" (直接责任人员) auferlegt werden. Die Höhe der Geldstrafe ist abhängig vom jeweiligen Verstoß und dessen Schwere und reicht von 10.000 Yuan bis 50.000.000 Yuan. Werden Korrekturen verweigert oder liegen erschwerende Umstände vor, wird meistens der Rahmen für Geldstrafen erhöht und es können zusätzliche Anordnungen getroffen werden. Dazu zählen: die vorübergehende Einstellung betreffender Geschäftstätigkeiten, Betriebsstilllegung zur Korrektur, die Annullierung betreffender betrieblicher Genehmigungen oder der Gewerbeerlaubnis.

Bei mildernden Umständen kann gemäß § 59 NetzwDatenSichVO nach den Bestimmungen des „Verwaltungsstrafgesetzes der Volksrepublik China"[35] verfahren werden und demnach die Sanktion gemildert, gemindert oder von ihr abgesehen werden.

34 Für Einzelheiten empfiehlt sich ein Blick in die jeweiligen Rechtsgrundlagen. Diese sind: §§ 59–72 NetzwSichG, §§ 45–48 DatenSichG, § 66 PersDatenSchG, §§ 55–58 NetzwDatenSichVO.

35 中华人民共和国行政处罚法 vom 27.8.2009 in der Fassung vom 22.1.2021, deutsch in der Fassung vom 17.3.1996 in: *Robert Heuser*, Sozialistischer Rechtsstaat und Verwaltungsrecht in der VR China (1982–2002), Hamburg 2003, S. 406 ff.

3. Haftung

Die untersuchten Rechtsquellen enthalten im Übrigen eine Klarstellung zum Verhältnis zur sonstigen Haftung. Entsteht einem anderen durch Verstoß gegen Bestimmungen ein Schaden, kann nach dem Recht die zivilrechtliche Haftung verfolgt werden (§ 74 Abs. 1 NetzwSichG, § 52 Abs. 1 DatenSichG, § 69 Abs. 1 PersDatenSchG, § 61 Hs. 1 NetzwDatenSichVO). Bilden die Verstöße Handlungen gegen die „Verwaltung öffentlicher Sicherheit" (治安管理), werden nach dem Recht Sanktionen zur Sicherheitsverwaltung verhängt[36] und bei Straftaten diese nach dem Recht verfolgt (§ 74 Abs. 2 NetzwSichG, § 52 Abs. 2 DatenSichG, § 71 PersDatenSchG, § 61 Hs. 2, 3 NetzwDatenSichVO).[37]

An einigen Stellen wird zudem die gesamtschuldnerische Haftung angeordnet, etwa bei gemeinsamer Verarbeitung (§ 20 Abs. 2 PersDatenSchG). Gemeinsam haften gemäß § 40 Abs. 3 NetzwDatenSichVO auch Netzwerkplattformendiensteanbieter mit Drittanbietern von Waren und Diensten.

Im Hinblick auf zivilrechtlichen Schadensersatz wird bei der Verarbeitung persönlicher Daten gemäß § 69 Abs. 1 PersDatenSchG das Verschulden des Verarbeiters widerlegbar vermutet. Die Höhe des Schadensersatzes richtet sich gemäß § 69 Abs. 2 Hs. 1 PersDatenSchG nach dem Schaden des Betroffenen oder dem durch den Verarbeiter erlangten Nutzen. Sind Schaden und Nutzen schwierig zu bestimmen, richtet sich die Höhe gemäß dessen Hs. 2 nach den tatsächlichen Umständen.

X. Fazit

Die Vielzahl der hier betrachteten Pflichten greift an unterschiedlichen Stellen auf verschiedene Art und Weise ineinander. Darin lässt sich das größte Problem der untersuchten Rechtsquellen erblicken. Es werden verschiedene Begriffe verwendet, die zwar viele Schnittmengen aufweisen, jedoch meist nicht völlig deckungsgleich sind. Am besten lässt sich das etwa am Verhältnis von Netzwerkdaten zu den übrigen Datenarten erkennen. Das macht es für Rechtsanwendende schwierig, den Überblick zu behalten. Die Überprüfung der eigenen Compliance macht es daher erforderlich, alle untersuchten Rechtsquellen parallel im Blick zu haben. Dieser Aufsatz gibt dafür eine systematische Hilfestellung an die Hand, die vor allem das Auffinden der relevanten Normen und der in ihnen niedergeschriebenen Pflichten erleichtern soll.

36 Nach dem „Gesetz der Volksrepublik China über die Strafen zur Regelung der öffentlichen Sicherheit" (中华人民共和国治安管理处罚法) vom 28.8.2005 in der Fassung vom 26.10.2012; abgedruckt in der Fassung vom 26.10.2012 in: Amtsblatt des Ständigen Ausschusses des Nationalen Volkskongresses (中华人民共和国全国人民代表大会常务委员会公报) 2012, Nr. 6, S. 693 ff.

37 Für den strafrechtlichen Schutz von Daten ist auf die aktuelle Fassung des chinesischen Strafgesetzes und einschlägige justizielle Interpretationen des Obersten Volksgerichts zu verweisen.