

The background of the top half of the cover is a vibrant yellow-green gradient. It features a grid of thin white lines. Diagonal bands of binary code (0s and 1s) are scattered across the grid, some appearing to flow from the top-left towards the bottom-right. There are also some faint, larger-scale grid lines and a few small white dots.

Datenrechtsgesetz 2.0

Die Systemkonstruktion der Datenrechte

Das Schlüssellabor für Big Data-Strategie

Herausgegeben von Lian Yuming

Peter Lang

Menschenrechte, Sachenrechte und Datenrechte sind drei grundlegende Rechte des künftigen Lebens der Menschheit. Das Datenrecht ist im Wesentlichen das Teilhaberecht. Es bedeutet die effiziente Nutzung von Daten und ist die endgültige Manifestation des Dateneigentumsrechts. Es hat besondere Bedeutung für das künftige Leben der Menschheit.

– People.cn

Die digitale Zivilisation stellt den Wertursprung und die treibende Kraft der Innovation für die Entstehung des Datenrechtgesetzes bereit, während das Datenrechtgesetz auch Grundlage für die Existenz des Ordnungssystems und Ordnungszuwachses der digitalen Zivilisation bietet.

– Demokratie und Rechtssystem Times

Die Forschung über das Datenrechtgesetz ist eine bahnbrechende und epochemachende Arbeit. Sie ist eine wichtige und große soziale oder akademische Frage, die die Nachkommen auf keinen Fall umgehen können.

– China-Afrika Tageszeitung

In diesem Sinne ist das Datenrechtgesetz ein Produkt des Sprungs unserer Zivilisation und der Evolution der Ordnung. Es ist ein wichtiger Grundstein auf dem Weg von der industriellen zur digitalen Zivilisation.

– eztv.vip

Der Vorschlag des Datenrechtgesetzes hat die rechtsstaatliche Grundlage für Aufrechterhaltung der nationalen Datensouveränität, für Festhaltung des Regelsetzungsrechts und internationalen Diskursrechts im Bereich der Datenrechte und für globale rechtsordnungsmäßige Cyberspace-Governance geschaffen. Er ist von besonderer Bedeutung für Förderung des Aufbaus einer Schicksalsgemeinschaft im Cyberraum.

– World Chinese Weekly



Datenrechtsgesetz 2.0

- Schwerpunktforschungsprojekt des Schlüssellabors für Big Data-Strategie
- Schwerpunktprojekt der wissenschaftlichen Stadtforschung des Schlüssellabors der Stadt Beijing auf der Grundlage der Big Data
- Projekt mit Förderung vom Verlagsfonds für Think Tank Engineering der Stiftung für internationalen Stadtkulturaustausch Beijing

Datenrechtsgesetz 2.0

Die Systemkonstruktion
der Datenrechte

Das Schlüssellabor für Big Data-Strategie

Herausgegeben von Lian Yuming



社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS(CHINA)



PETER LANG

Oxford • Bern • Berlin • Bruxelles • New York • Wien

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available on the Internet at <http://dnb.ddb.de>.

A catalogue record for this book is available at the British Library.

Cover design: Brian Melville for Peter Lang

ISBN 978-1-80079-430-6 (print) • ISBN 978-1-80079-431-3 (ePDF)

ISBN 978-1-80079-432-0 (ePub) • ISBN 978-1-80079-433-7 (mobi)

DOI 10.3726/b18355

PETER LANG



Open Access: This work is licensed under a Creative Commons Attribution

Non Commercial No Derivatives 4.0 unported license. To view a copy of this license,
visit <https://creativecommons.org/licenses/by-nc-nd/4.0/>

© Lian Yuming 2021

Published by Peter Lang Ltd, International Academic Publishers,
52 St Giles, Oxford, OX1 3LU, United Kingdom
oxford@peterlang.com, www.peterlang.com

Lian Yuming has asserted his right under the Copyright, Designs and Patents Act, 1988,
to be identified as Editor in Chief of this Work.

This publication has been peer reviewed.

*Wissenschaftliche Unterstützung durch
Forschungsbasis des Schlüssellabors für Big-Data-Strategie der
Chinesischen Universität für Politikwissenschaft und Recht
und
Forschungszentrum für Datenrechtsgesetz
der Chinesischen Universität für Politikwissenschaft und Recht*

Vorstellung der Institution

Das Schlüssellabor der Big-Data-Strategie wurde im April 2015 gegründet und ist eine interdisziplinäre, professionelle, internationale und offene Forschungsplattform, die von der Volksregierung der Stadt Guiyang und der Stadtkommission für Wissenschaft und Technik Peking mitbegründet wurde. Es ist zudem eine neuartige, hochrangige Denkfabrik, die sich mit der Entwicklung von chinesischem Big Data befasst.

Unter Berufung auf den Rat der Global City Development Corporation in Peking und das Forschungsinstitut für innovationsgetriebene Entwicklungsstrategie in Guiyang richtete das Schlüssellabor für Big-Data-Strategie zwei Forschungszentren in Peking und Guiyang ein. Außerdem werden fünf Forschungsbasen eingerichtet: die Forschungsbasis der zentralen Parteischule, die Forschungsbasis des Nationalen Komitees für Begriffe in Wissenschaft und Technologie Chinas, die Forschungsbasis der Zhejiang-Universität, die Forschungsbasis der Chinesischen Universität für Politikwissenschaft und Recht und die Forschungsbasis der Akademie der Wissenschaften Shanghai. In der Provinz Guizhou wurde die Einrichtung von drei Forschungsplattformen genehmigt, nämlich die Plattform für Forschung der Blockdatentheorie und angewandte Innovation, die Plattform für angewandte Big-Data-Innovationsforschung für Stadtraumentscheidungen und die Forschungsplattform für Big-Data-Innovation in der Kultur. Die Struktur „zwei Zentren, fünf Forschungsbasen und drei Forschungsplattformen“ schafft ein neues Forschungssystem und ein regionales kollaboratives Innovationsmuster.

Das Schlüssellabor für Big-Data-Strategie hat folgende wichtige innovative Ergebnisse in Big-Data-Entwicklungstheorien und Praxis veröffentlicht: *Blockdaten: Das Signal der Ankunft der Big-Data-Zeit*, *Blockdaten 2.0: Paradigmenrevolution im Zeitalter von Big Data*, *Blockdaten 3.0: Das Ordnungs-Internet und souveräne Blockchains*, *Blockdaten 4.0: Aktivierungsdaten im Zeitalter der künstlichen Intelligenz*, *Blockdaten 5.0: Theorien und Methoden der Datensoziologie*, *Datenrechtsgesetz 1.0: Theoretische*

Grundlagen des Datenrechts (in Chinesisch, Englisch, Französisch, Deutsch und traditionellem Chinesisch), Souveräne Blockchain 1.0: Ordnungs-Internet und die Schicksalsgemeinschaft der Menschheit, Blaubuch Big Data – Jahresbericht zur Entwicklung von Big Data in China (Nr. 1 – Nr. 4) und hat im In- und Ausland einen erheblichen Einfluss ausgeübt.

Vorstellung des Chefredakteurs

Lian Yuming, Professor und Doktor in Engineering, Mitglied des Nationalkomitees der politischen konsultativen Konferenz des chinesischen Volks, Präsident des Peking Forschungsinstituts für internationale Stadtentwicklung und Direktor des Forschungszentrums für das Datenrechtsgesetz der China Universität für Politikwissenschaft und Rechte.

Lian Yuming ist ein renommierter Experte für Stadtentwicklung in China. Er ist der stellvertretende Vorsitzende der Pekinger Volkskonsultativkonferenz des Chaoyang-Bezirks, Mitglied des Expertenkonsultativausschusses der Volksregierung von Peking, der stellvertretende Vorsitzende des Pekinger Verbandes der Sozialwissenschaftlichen Kreise, der Hauptexperte in der Forschungsbasis der in Peking, Tianjin, Hebei koordinierten Entwicklung sowie der Direktor des Pekinger Schlüssellabors für Stadtforschung auf der Basis von Big Data. Seine Forschungsschwerpunkte sind Urbanologie, Entscheidungswissenschaft und Soziologie. Zu seinen Hauptwerken gehören die Veröffentlichungen *Entstehung von Städten*, *Strategische Positionierung Pekings und Wiederentdeckung der Weltstädte*.

Im März 2014 übernahm Prof. Lian eine vorübergehende Position als Assistent des Bürgermeisters der Stadtregierung von Guiyang und wurde zum Präsidenten des Forschungsinstituts für innovationsgetriebene Entwicklungsstrategie in Guiyang und zum Leiter des Schlüssellabors für Big-Data-Strategie ernannt. Fortan forschte er über die Big-Data-Strategie und veröffentlichte Bücher wie *Block Data: Das Signal der Ankunft von Big Data Time*, *Block Data 2.0: Paradigmenrevolution im Zeitalter von Big Data*, *Block Data 3.0: Ordnungs-Internet und Souveränes Blockchain*, *Block Data 4.0: Aktivierungsdaten im Zeitalter der künstlichen Intelligenz*, *Block Data 5.0: Theorien und Methoden der Datensoziologie*, *Datenrechtsgesetz 1.0: Theoretische Grundlagen des Datenrechts (in Chinesisch, Englisch, Französisch, Deutsch und traditionellem Chinesisch)*, *Souveräne Blockchain 1.0: Ordnungs-Internet und die Schicksalsgemeinschaft der Menschheit*, *Blaubuch Big Data: Jahresbericht zur Entwicklung von Big Data in China (Nr. 1-4) usw.*

Redaktionsausschuß

Hauptberater:	Chen Gang, Yan Aoshuang
Direktor:	Zhao Deming
Exekutiver Direktor:	Chen Yan
Stellvertretender direktor:	Xu Hao, Liu Benli, Lian Yuming
Chefredakteur:	Lian Yuming
Stellvertretender Chefredakteur:	Long Rongyuan, Zhang Longxiang
Hauptforscher:	Lian Yuming, Zhu Yinghui, Song Qing, Wu Jianzhong, Zhang Tao, Song Xixian, Long Rongyuan, Zhang Longxiang, Zou Tao, Shen Xudong, Chen Wei, Yang Guanhua, Yang Lu, Yang Zhou
Wissenschaftlicher Sekretär:	Li Ruixiang, Long Wanling

Übersetzungsausschuß

Übersetzer:

Zhang Yuhui

Lektor:

Zhou Hongjing

INHALTSVERZEICHNIS

Vorwort des Chefredakteurs	xvii
Einleitung	xxvii
KAPITEL 1	
Datenperson	1
Abschnitt I Menschliche Basis des Gesetzes	2
Abschnitt II Datenperson-Hypothese und Altruismus	21
Abschnitt III Das Datenrechtssystem und die Legalisierung von Datenrechten	38
KAPITEL 2	
Datenrecht	63
Abschnitt I Datenrecht und Datenmacht	64
Abschnitt II Type der Datenrechte	86
Abschnitt III Konfrontation im Rahmen der Datenrechte	105
Abschnitt IV Schutz der Datenrechte	120
KAPITEL 3	
Teilhaberechte	143
Abschnitt I Gesetzliche Begründung der Teilhaberechte	143
Abschnitt II Ansprüche auf das Teilhaberecht	164
Abschnitt III Inhalt der Teilhaberechte	178
Abschnitt IV Wert der Teilhaberechte	196
KAPITEL 4	
Datensouveränität	211
Abschnitt I Aufstieg der Datensouveränität	212
Abschnitt II Rechtsposten der Datensouveränität	229

Abschnitt III	Spiel der Datensouveränität	244
Abschnitt IV	Verwaltung der Datensouveränität	257
KAPITEL 5		
	Datenrechtssystem: Ein internationaler Vergleich	277
Abschnitt I	Datenrechtssysteme des Auslandes	278
Abschnitt II	Chinas Datenrechtssystem	312
Abschnitt III	Sonderbedeutung des Datenrechtssystems für die globale Internetverwaltung	346
	Nachwort	367
	Nomenklatur	373

Vorwort des Chefredakteurs

Während der gesamten Geschichte der Weltzivilisation hat die Menschheit die landwirtschaftliche Revolution, die industrielle Revolution und die Informationsrevolution erlebt. Jede technologische Revolution hat enorme und tief greifende Auswirkungen auf die menschliche Produktion und das Leben gehabt. Die anhaltende Datenrevolution verändert unser Leben in ähnlicher Weise und sogar noch umformender. Überwältigende Veränderungen herbeizuführen, bedeutet nicht bloß eine ergänzende Erweiterung oder eine einseitige Ausdehnung unserer Welt, sondern in großem Maße einen allseitigen Ersatz der Produktions-, Lebens- und Existenzweisen der Menschheit seit der industriellen Revolution. Mit der Entwicklung der digitalen Wirtschaft und dem Fortschritt des unbemannten Fahrens, der Genbearbeitung und anderer neuer Technologien entstehen weiterhin neue Arten von Rechtsbeziehungen. Die Erfahrungen, die die Menschheit im Laufe der Zeit gesammelt hat, und die Regeln, die heute in der Gesellschaft angewendet werden, werden schwer gestört und umstrukturiert. Wie ein Sprichwort eines alten Nomadenstamms betont: „Ihre Seele würde nicht mithalten können, wenn Sie zu schnell gehen.“ Wir können dieses Sprichwort auch verwenden, um die reale Situation zu beschreiben, mit der wir jetzt konfrontiert sind: Wenn wir bei der Entwicklung und Nutzung von Big Data zu schnell Fortschritte machen, werden versteckte Probleme und lokale Unordnung häufig auftauchen. Während derzeit die Welt digitalisiert, vernetzt und intelligent wird, sind die Verständnisse für die digitale Welt durch die traditionellen Rechtsgrundsätze und die Gesetzgebungsweise auf schwierige theoretische Dilemma und praktische Schwachstellen gestoßen. „Wenn Gesetze an die Zeit angepasst werden, gibt es eine gute Regierung.“ Das Gen von „Big Data“ soll bei der Schaffung und Entwicklung des neuen Rechtssystems implantiert werden, damit wir zukunftsweisende Theorien und innovative Systeme für den dreifachen Raum, den die Menschheit betritt, etablieren

und auf die bevorstehende Ära der digitalen Zivilisation Vorbereitungen treffen können.

I. Drei Voraussetzungen für die Datenperson-Hypothese

Der Mensch ist der logische Ausgangspunkt des Gesetzes, und das Gesetz ist die Manifestation der menschlichen Natur. Die Rechtsgrundlage des Datenrechtsgesetzes liegt in der menschlichen Natur. Deshalb sollte das System des Datenrechtsgesetzes auch aus der menschlichen Natur hervorgehen. Daher ist es notwendig, dass wir unsere Gesetze und ihre Anwendung unter dem Gesichtspunkt der menschlichen Natur gestalten. Die menschliche Natur ist durch ihre Offenheit und Entwicklung charakterisiert. Nur wenn wir unser Image ständig erneuern und neue Vorschriften schaffen, können wir Menschen unsere eigenen Widersprüche auflösen und uns vervollkommen. Die "Datenperson" ist eine neue Manifestation der menschlichen Natur im Zeitalter von Big Data. Wir können nur die Grundlage für die Legitimität des Datenrechtsgesetzes aus der Perspektive von Datenethik legen, wenn wir das Modell der Rechtsperson für Datenperson sowie den Weg, Umfang und die Ausdrucksweise für das Datenrechtssystem festlegen. Die Begründung der Datenperson-Hypothese für das Datenrechtsgesetz liegt darin, dass sie sowohl die neue Anschauung der menschlichen Natur, die von den grundlegenden Merkmalen wie Altruismus und Gemeinnutzung usw. bestimmt ist und die von relevanten Subjekten gebührenderweise gezeigt werden sollte, beschreiben kann, als auch dazu führen, das Datenrechtsgesetz auf wissenschaftlich fundierte Weise zu erlassen und es effektiv umzusetzen, indem die schwierige Lage der Sicherheit bei der Datenverwaltung gemildert oder überwunden wird. Zugegebenermaßen gibt es jedoch Voraussetzungen für die Existenz und Entwicklung der Datenperson-Hypothese.

Die Abhängigkeit von Dingen geht zur Abhängigkeit von Daten über. Die Daten zeigen und beschreiben das gesamte Leben eines jeden Menschen von der Wiege bis zum Grab. Wir sind heute untrennbar von Daten abhängig. Und diese Abhängigkeit der Menschen von „Daten“ entsteht zu

einer Zeit, in der wir noch nicht ganz frei von Abhängigkeit von anderen Personen und Dingen sind. Das Bild, die Konnotation und die Epitaxie des „Menschen“ werden sich grundlegend ändern, wenn die digitalisierte Produktion, das digitalisierte Leben und die digitalisierte Art und Weise, wie wir unser Leben führen, realisiert werden, wenn sich die menschliche Intelligenz und künstliche Intelligenz verschmelzen und wenn sich die „natürliche Person“ dann zu „Datenperson“ entwickelt. Weder die Entwicklung der Technologie noch die Kette der Evolution haben ein Ende. Ganz möglicherweise könnte die menschliche Gesellschaft in Zukunft aus „natürlichen Personen“, „Robotern“ und „Gen-editierten Menschen“ bestehen. Es soll darauf hingewiesen werden, dass der Status der „Datenperson“ eine rechtliche Frage ist, der wir uns in Zukunft stellen müssen.

Der Altruismus ist in das Fundament unserer Gesellschaft eingewoben. Die Struktur der Beziehungen in der digitalen Gesellschaft bestimmt, dass der innere Mechanismus einer solchen Gesellschaft dezentralisiert, abgeflacht und grenzenlos ist und die Grundgedanken von Offenheit, Teilhabe, Zusammenarbeit und gegenseitigem Nutzen aufweist. Diese Merkmale bedeuten, dass die Grundierungsfarbe unserer Gesellschaft „menschenorientiert“ sein wird und der Altruismus als Kernwerte in dieser Ära gilt. Die Wertansicht des Altruismus erhöht die Bereitschaft der Menschen, Datenrechte zu übertragen und an Daten teilzuhaben, und so verwandelt diese Übertragung und Teilhabe in Verhaltensweisen, die in der Gesellschaft positiv wahrgenommen werden. Wenn die Datenressourcen und -produkte äußerst reichlich vorhanden sind und je nach Bedarf zugewiesen werden können, wird die Idee der gleichberechtigten Teilhabe in den menschlichen Herzen wurzeln, die Datenarbeit zu einem Weg zum glücklichen Leben und der Altruismus sich erheblich zunehmen und verbreiten. Bis dahin würde der Altruismus, der sich in der menschlichen Natur verbirgt, entfesselt und das Datenrechtssystem würde auch in gewissem Maße die Rolle einer altruistischen „Hebamme“ spielen.

Die Datenperson maximiert den Datenwert. Sie betrachtet die Wertmaximierung als das ultimative Ziel, schafft und realisiert den Datenwert, wobei sie das grundlegende Prinzip der Wertmaximierung verfolgt. Als Rechtssystem für Regulierung von Zugehörigkeit, Rechten, Nutzung und den Schutz von Datenrechten und als Grundregeln für Vorschriften über

die datenbezogene Verhaltensweise und Aufrechterhaltung der Datenordnung in der Datenwelt zielt das auf der Datenperson-Hypothese basierende Datenrechtssystem hauptsächlich darauf ab, ein Gleichgewicht und eine Koordinierung zwischen dem wirksamen Schutz der Datenrechte und der bestmöglichen Nutzung der Daten zu erreichen, die öffentlichen Interessen und öffentliche Sicherheit zu wahren und die freie Teilhabe an personenbezogenen Daten zu fördern. Zum Zweck des Gleichgewichts und Koordinierung zwischen dem legalen Schutz und der rationellen Nutzung von Daten ist die Übertragung von Datenrechten durch Bürger bis zu einem gewissen Grad von entscheidender Bedeutung. Das heißt, das Ziel der Gesetzgebung zu Datenrechten soll den Datenverkehr und die Datennutzung fördern, anstatt Beschränkungen des Datenverkehrs über eine dichte gesetzliche Masche aufzuerlegen. Die Entstehung eines soliden Datenrechtssystems bedeutet, dass die Menschheit die Beziehungen zwischen Menschen und Daten besser verstanden hat und dass wir den Datentransfer zum Wohl der Gesellschaft befürworten.

2. Drei Rechte und Interessen im Zeitalter von Big Data

Im Laufe der Zeit müssen wir ständig neue Rechte anerkennen, um den Bedürfnissen der Gesellschaft gerecht zu werden. Angesichts der rasanten Digitalisierungsflut müssen wir ein auf Datenrechten basierendes Rechtesschutzsystem aufbauen, um einen umfassenden Datenschutz zu erreichen. Datenrechte, das Teilhaberecht und die Datenhoheit sind neue Rechte und Interessen im Zeitalter von Big Data. Diese Rechte und Interessen sind berechtigt, in Liste der gesetzlichen Rechte aufgenommen zu werden. In gewissem Sinne kann man sagen, dass die Entstehung der Datenrechte im Laufe der Entwicklung der Gesellschaft unserem Rechtssystem eine Möglichkeit zur Verbesserung und Vervollständigung gebracht hat.

Datenrechte. Daten haben die Tendenz zu einer Art von Ressource, zur Assetisierung und Kapitalisierung. Gleichzeitig treten Rechtsverletzung oder Delikt im Zusammenhang mit Datenrechten wie illegale Erhebung,

Diebstahl, Handel und Missbrauch von Daten etc. immer häufiger auf. Die Stärkung der gesetzlichen Unterstützung für den Schutz, die Entwicklung und Nutzung von Daten durch Einrichtung eines soliden Rechtssystems ist eine wichtige Agenda für Gesetzgeber in verschiedenen Ländern der Welt sowie für Forscher aus dem In- und Ausland, die die „Datenrechte“ als Bezeichnung ihrer Forschungsthemen betrachten. Als separate Kategorie neu entstehender Rechte umfassen Datenrechte wie personenbezogene Datenrechte, Unternehmensdatenrechte und Regierungsdatenrechte etc. Der Schutz von Datenrechten ist ein übergreifender Begriff, der die Datenrechte im privatrechtlichen Sinne und Datenmacht im Sinne öffentlicher Gewalt abdeckt. Der Kern der Rechtsstaatlichkeit besteht darin, die öffentliche Macht zu regeln, die privaten Rechte zu schützen, die Gerechtigkeit zu wahren und der Gesellschaft Orientierung zu geben. Als Erweiterung der traditionellen privaten Rechte und öffentlichen Macht im digitalen Raum haben Datenrechte und Datenmacht jetzt häufigere Konflikte. Gegenwärtig wachsen sowohl Datenrechte als auch Datenmacht rasant. Auf lange Sicht werden die Verbreitung von Datenrechten und der Rückgang der Datenmacht der unvermeidliche Trend sein.

Teilhaberechte. Durch Teilhabe werden Daten effektiver genutzt. Sie ist die ultimative Repräsentation des Dateneigentumsrechts. Im Gegensatz zu den dinglichen Rechten sind Datenrechte kein Besitzrecht mehr, sondern zu einer Art von nichtexklusiven Teilhaberechten, was bedeutet, dass die „Daten in der Regel mehrere Eigentumsrechte haben“. Sobald Datenrechte von einem natürlichen Recht zu einem öffentlichen Recht und einem allgemeinen Willen aufgewertet werden, gehen sie unweigerlich über das hinaus, was durch ihre Form ausgestattet ist und werden zu einem sozialen Recht. Das Teilhaberecht ist das Wesen der Datenrechte und wird über Nutznießdatenrechte und Nutznießdatenrechte der öffentlichen Interessen verwirklicht. Auf diese Weise wird es möglich, das Datennutzungsrecht vom Dateneigentumsrecht zu trennen und ein grundlegendes Muster für Teilhabe zu bilden, bei dem man Daten „nicht besitzen, sondern nur nutzen“ will. Aufgrund des Spiels zwischen öffentlichen und persönlichen Interessen und der Diskrepanz zwischen Eigentumsinteressen und Persönlichkeitsinteressen bestehen natürliche Interessenkonflikte zwischen Datenteilhabe und Schutz der Privatsphäre.

Daher muss ein Gleichgewicht zwischen dem Teilhaberecht und dem Recht auf Privatsphäre hergestellt werden, um den Wert der Datenressourcen vollständig zu erforschen. Mit dem Vorschlag für Teilhaberecht initiieren wir eine neue Regel der Rechtstheorie, die über das Sachenrecht hinausgeht und auch kennzeichnende Bedeutung für die digitale Zivilisation hat. Es ist absehbar, dass die menschliche Zivilisation auf der Grundlage der Teilhabe auf eine höhere Ebene gelangt und in eine neue Ordnung eintritt, die auf den Teilhaberechten aufgebaut wird.

Datensouveränität. Der digitale Raum ist nach Land, Meer, Luft und Raum das „fünfte Territorium“ geworden. Die Datenbestände, die ein Land in seinem Besitz hat, wie aktiv die Daten sind und die Fähigkeit des Landes, die Daten zu interpretieren und zu verwenden, werden zu einem wichtigen Bestandteil der umfassenden nationalen Stärke des Landes. Der Begriff der Datensouveränität ist von den geographischen Elementen losgelöst, da die Datenhoheit einen neuen Begriffszweig bildet und zu einem zentralen Bestandteil des gesamten Souveränitätssystems wird. Die Datenhoheit ist ein wichtiger Bestandteil der nationalen Souveränität und eine Verkörperung und natürliche Erweiterung der nationalen Souveränität im Datenraum. Wenn die Datenmacht den Hauptindikator für die umfassende nationale Stärke und internationale Wettbewerbsfähigkeit eines Landes darstellt, wird die Datenhoheit dann zur Voraussetzung und Grundlage für Wahrung der Kerninteressen eines Landes. Länder der ganzen Welt haben begonnen, eigene Datenhoheitssysteme einzurichten, um Daten besser zu verwalten und kontrollieren zu können. Beispielsweise hat die Europäische Union die „Allgemeine Datenschutzverordnung“ eingeführt, damit die extraterritoriale Zuständigkeit für Daten beansprucht wurde. Die Vereinigten Staaten haben den „Clarifying Lawful Overseas Use of Data Act“ herausgegeben, dadurch der Strafverfolgungsbehörde das Recht eingeräumt wird, extraterritoriale Daten zu erhalten. Das Russland hat das „souveräne Internetgesetz“ verabschiedet, um eine „autonome und kontrollierbare“ Cyber-Souveränität über das russische Netzwerk zu etablieren. Länder wie Australien, Brasilien, Kanada, Indien und Südkorea usw. haben ähnliche Gesetze gegeben. Bisher ist die Datenhoheit ein neues Maß für das globale Spiel und den internationalen Wettbewerb geworden.

3. Drei große Einflüsse des Datenrechtsgesetzes

Die heutige Welt befindet sich inmitten radikaler Veränderungen, die wir in den letzten 100 Jahren noch nie gesehen haben. Die menschliche Gesellschaft steht sowohl vor guten Hoffnungen als auch vor heftigen Herausforderungen. Wie Stephen Hawking so ausdrückte: „Wir stehen an der Schwelle einer schönen neuen Welt. Und das ist ein aufregender wie aber auch prekärer Ort, an dem man sein kann ...“ Das Spiel um die Einrichtung eines globalen Cyberspace-Verwaltungssystems verschärft sich immer mehr, da im Verwaltungsprozess zahlreiche Schwierigkeiten auftreten und weitere Meinungsverschiedenheiten hinsichtlich des Verwaltungsmodells bestehen. Obwohl die Länder der Welt unterschiedliche nationale Bedingungen haben, sich in unterschiedlichen Stadien der Internetentwicklung befinden und unterschiedlichen Herausforderungen gegenüberstehen, haben wir aber den gleichen Wunsch und Interessen, die Entwicklung der digitalen Wirtschaft zu fördern, die Herausforderungen der Cybersicherheit anzugehen und die Verwaltung des Cyberspace zu stärken. Das Datenrechtsgesetz ist ein neuer Ansatz für die globale Cyberspace-Verwaltung, der von China vorgeschlagen worden ist. Es bietet die chinesische Weisheit und chinesische Lösungen für Schaffung einer Schicksalsgemeinschaft im Cyberspace.

Das Datenrechtsgesetz ist ein wichtiges Symbol dafür, dass die chinesische Gesetzgebung die Weltbühne betreten hat. China befindet sich derzeit in den umfassendsten und tief greifendsten sozialen Veränderungen in der Geschichte der Menschheit und arbeitet an den ehrgeizigsten und einzigartigsten rechtsstaatlichen innovativen Praktiken. Ein solides Rechtssystem ist das Rückgrat des nationalen Verwaltungssystems. Präsident Xi Jinping erklärte: „China muss die Rechtsstaatlichkeit gut nutzen, wenn es mit der Welt interagiert und als ein wichtiges und verantwortungsbewusstes Land an internationalen Angelegenheiten teilnimmt ... Das Global-Verwaltungssystem befindet sich in einer Schlüsselphase der Anpassungen und Veränderungen. Wir sollen uns aktiv an der internationalen Regelsetzung beteiligen und Teilnehmer, Förderer und Verfechter der Transformation der globalen Verwaltung sein.“ Das Datenrechtsgesetz

als Innovation und Durchbruch auf dem Gebiet des Rechts ist wegweisend und fördert Fortschritte bei der Globalisierung von Recht und Rechtswissenschaft. Insbesondere die Veröffentlichung unserer Buchreihe zum Datenrechtsgesetz in mehreren Sprachen präsentiert der Welt chinesische Ideen, gibt die chinesische Stimme und schlägt chinesische Lösungen für die globale Cyberspace-Verwaltung vor. Das ist ein wichtiges Zeichen dafür, dass China den Aufstieg der chinesischen Gesetze und ihren Schritt in den Mittelpunkt der Weltbühne einläutet. Das ist auch ein wirksames Rechtsinstrument für Chinas Beteiligung an der globalen Verwaltung im Zeitalter der digitalen Zivilisation und auch ein Ereignis als Meilenstein in unseren Bemühungen für Bereitstellung von öffentlichen Produkten für die globale Verwaltung.

Das Datenrechtsgesetz ist ein wichtiger Bestandteil der künftigen Rechtsstaatlichkeit. Wenn eine weitere große soziale Revolution in der menschlichen Gesellschaft vor der Tür steht, wird es eine Revolution in der Gesetzgebung geben, die eine bessere Regelführung für das digitale Imperium anstrebt. In der heutigen Welt mit Verwaltung in verschiedenen Formen, auf mehreren Ebenen und in verschiedenen Bereichen hat sich unser Verwaltungsmodell schrittweise an diese Ära der Globalisierung angepasst. Wenn das Verwaltungssystem jedoch komplexer wird, kann seine Wirksamkeit und Legitimität leicht beeinträchtigt werden. Um Konflikte in Bezug auf die Datenhoheit zu vermeiden, sollen wir durch internationale Zusammenarbeit internationale Regeln formulieren, ein Datenrechtssystem einrichten und eine internationale Rechtsgemeinschaft gestalten. Das ist ein möglicher Pfad, damit die Menschheit auf der Grundlage des Rechtssystems eine Schicksalsgemeinschaft im Cyberspace bauen kann. Mit Blick auf die Entwicklung der Rechtsstaatlichkeit in der Welt ist es nicht schwer, einen Trend der Integration und globalen Vereinheitlichung zwischen Gesetzen aus verschiedenen Teilen der Welt zu erkennen. Gegenwärtig versuchen wir, uns Rechtsstaatlichkeit für die Zukunft vorzustellen, damit wir herausfinden können, welche Optionen wir heute haben, um die künftige Rechtsstaatlichkeit besser zu verstehen. Das Datenrechtsgesetz bietet Einblicke in die künftigen Gesetze und regt unsere endlosen Vorstellungen an.

Das Datenrechtsgesetz ist ein wichtiger Grundstein auf dem Weg der Menschheit zur digitalen Zivilisation. „In der Vergangenheit war das Gesetz

ein Produkt der Zivilisation. Derzeit ist das Gesetz ein Werkzeug, mit dem wir die Zivilisation am Laufen halten. Für die Zukunft ist das Gesetz ein Mittel, mit dem wir die Zivilisation vorantreiben.“ Als die menschliche Gesellschaft von der landwirtschaftlichen zur industriellen und dann zur digitalen Zivilisation übergeht, springt das Gesetz vom „Gesetz des Menschen“ zum „Gesetz der Dinge“ und dann zum „Gesetz der Daten“. Die digitale Zivilisation bietet die Wertbegründung und treibende Kraft bei der Schaffung des Datenrechtsgesetzes, während das Datenrechtsgesetz Grundlage für die Existenz der digitalen Zivilisation zur Aufrechterhaltung ihrer Systeme und zur Verbesserung ihrer Ordnung liefert. Die Bedeutung des Datenrechtsgesetzes konzentriert sich auf das Ordnungsparadigma der digitalen Zivilisation und bildet die Basis für Aufrechterhaltung der Ordnung in dieser Zivilisation. In diesem Sinne ist das Datenrechtsgesetz ein Produkt des Sprunges unserer Zivilisation und auch ein Grundstein für den Vormarsch der Menschheit von der industriellen zur digitalen Zivilisation. Zusammen mit dem Sachenrechtsgesetz bildet es zwei große rechtliche Grundlagen für die Ära der digitalen Zivilisation.

Lian Yuming

Direktor des Schlüssellabors für Big-Data-Strategie

Direktor des Forschungszentrums für Datenrechtsgesetz an
der Chinesischen Universität für Politikwissenschaft und Recht

Peking, den 17. Januar 2020

Einleitung

Auf der heutigen Welt steht die Menschheit vor vielen beispiellosen Herausforderungen. Globale Bedenken in verschiedenlicher Form wie Atomkrieg, Cyberkrieg, Finanzkrieg, biologischer Krieg und nicht-souveräne Macht etc. plagen die Menschheit. Der Schlüssel für Lösung dieser globalen Probleme ist die globale Verwaltung. Und die Schicksalsgemeinschaft für die Menschheit ist der „Vorschlag von China“ in Bezug auf die helle Zukunft, menschliche Entwicklung und das globale Regieren. Die internationale Rechtsgemeinschaft stellt die rechtstaatliche Unterstützung für die Schicksalsgemeinschaft der Menschheit dar und existiert als ein gemeinsames Regelsystem in der interdependenten internationalen Gemeinschaft. Sie trägt dazu bei, die gemeinsamen Interessen verschiedener Länder zu erweitern, eine Interessengemeinschaft zu bilden und den internationalen Aktionsträgern die Erfüllung ihrer gemeinsamen Verantwortungen zu ermöglichen. Das Datenrechtsgesetz ist ein wichtiger Bestandteil dieser internationalen Rechtsgemeinschaft und stellt unsere Einblicke in die Entwicklungstrends der Technologie, der Gesetze und der Menschheit dar. Die Darstellung des Datenrechtsgesetzes ist ein wichtiges Symbol dafür, dass die chinesischen Gesetze aufragen und in die Mitte der Weltbühne marschieren und dienen auch als ein mächtiges Rechtsinstrument für Teilnahme von China an der globalen Verwaltung in der Ära der digitalen Zivilisation.

I

Auf der Eröffnungszeremonie der Jahreskonferenz 2017 des Weltwirtschaftsforums Davos hat Präsident Xi Jinping darauf hingewiesen: „Heute leben wir auch in einer Welt der Widersprüche. Einerseits

häuft der materielle Reichtum ständig an, die Wissenschaft und Technologie machen immer schnellere Fortschritte und die Entwicklung der menschlichen Zivilisation hat das höchste Niveau in der Geschichte erreicht. Andererseits spielen regionale Konflikte wiederholt ab. Die globalen Herausforderungen wie Terrorismus und Flüchtlingsströme passieren Welle auf Welle. Die Unsicherheiten wie Armut, Arbeitslosigkeit und die immer größer gewordene Einkommensschere etc., vor denen die Welt steht, nehmen immer zu“. Am nächsten Tag hat Präsident Xi Jinping bei seiner Rede im Hauptquartier Genf der UNO die Frage unserer Zeit aufgeworfen: „Was ist mit der Welt passiert und wie sollen wir darauf reagieren?“ Mehr als zwei Jahre später gab er bei der Abschlussfeier des von China und Frankreich gemeinsam veranstalteten Globalen Verwaltungsforums erneut seine Einblicke in die Weltsituation. „Die heutige Welt steht vor großen Veränderungen gegenüber, die man in einem Jahrhundert nie gekannt hat. Der Frieden und die Entwicklung bleiben immer das Thema der Zeit. Zugleich steht die Menschheit vor einer Vielzahl von gemeinsamen Herausforderungen, da Unsicherheiten und destabilisierende Faktoren immer weiter zunehmen“.

Die Welt steht vor Veränderungen und Herausforderungen, die die Menschheit seit hundert Jahren nicht erlebt hat. Eine davon ist die Bedrohung durch den Atomkrieg. Seit dem einundzwanzigsten Jahrhundert haben die großen Länder der Welt eines nach dem anderen nukleare Strategien gestartet und sich darauf konzentriert, ihre Kapazität für die nukleare Abschreckung sowohl mit defensiven als auch offensiven Fähigkeiten aufzubauen. Dies hat weltweit zu einem teuflischen nuklearen Wettbewerb und nuklearem Spiel geführt. Die teuflische nukleare Entwicklung könnte die strategische Stabilität der Welt weiter untergraben, was einen dritten Weltkrieg auslösen kann, der durch Atomwaffen gekennzeichnet ist und dadurch die Öffnung der „Büchse der Pandora“ der Menschheit ermöglicht. Die zweite Bedrohung kommt vom Cyberkrieg, der eine völlig neue Form der Kriegsführung aufweist. Der Cyberspace ist zu einem neuen Schlachtfeld geworden, wo Länder um Ergreifen, Kontrolle, Besetzen, Angriff und Verteidigung heftig kämpfen. Da der Cyberspace mit dem physischen Raum, in dem die Menschheit lebt, eng verbunden ist und auf

Gedeih und Verderb zusammenhält, stellt einen Cyberkrieg eine noch größere Bedrohung für die Menschheit dar als der Atomkrieg. Das stille und leise Auftauchen des Cyberkriegs könnte zu einer der Hauptursachen für Turbulenz und Unordnung in der Welt werden und die Menschheit in eine Welt der Unordnung hineinzwingen. Die dritte Bedrohung kommt aus dem Finanzkrieg. Die finanzielle Sicherheit ist wichtig für die wirtschaftliche Entwicklung und den Weltfrieden. Sie ist ein wichtiges Thema der globalen Verwaltung. Angesichts der Haupttendenz der Entwicklung der globalen wirtschaftlichen Integration würde eine systematische Finanzkrise in einem Land unweigerlich die Entwicklung der gesamten Weltwirtschaft schwerwiegend verwüsten und kaum ein Land kann aus ihr herauslassen, wenn irgendein Land einmal von einer solchen Finanzkrise getroffen wird. Die vierte ist Bedrohung durch biologische Kriegsführung. Die Menschheit steht heute vor zahlreichen gesundheitlichen Herausforderungen wie Krebs, Ebola und HIV/AIDS etc. sowie vor sozialen Risiken in verschiedenen Dimensionen, einschließlich der Entfremdung durch Genbearbeitung. Für natürliche Personen stellt der durch die Genbearbeitung geschaffene „Supermenschheit“ einen tödlichen dimensionsreduzierenden Schlag von der „fortgeschrittenen Zivilisation“ auf die „Zivilisation auf niedrigem Niveau“ dar. Sobald dieser seine Fassung verlöre, könnte die Menschheit in einer Katastrophe wie nie zuvor geraten. Die fünfte Bedrohung ist die nichtsoveränen Kräfte. Das „Democracy Network“ als nichtsoveräne Kräfte, die sich darauf konzentrieren, das Internet zu nutzen, um andere Länder zu demokratisieren. Dieses Netzwerk kann leicht über die nationalen Grenzen hinaus ein globales Netzwerk bilden, das souveräne Staaten beeinflusst und kontrolliert oder sogar bindet, und damit die internationale geopolitische Ordnung direkt oder indirekt verändert und zu einer globalen Gefahr neuer Art werden. Zusätzlich zu all diesen steht die Menschheit auch vor zwei „Graues Nashorn“-Ereignissen, die umstürzlerische Auswirkung haben und gegen die sogar kein Widerstand geleistet werden kann. Das eine ist die globale Erwärmung. Der jüngste UN-Bericht hat uns erneut vor Klimakatastrophen gewarnt, die eintreten könnten: Ende dieses Jahrhunderts würde der Meeresspiegel möglicherweise um ein Meter ansteigen und Katastrophen wie extreme Wetter, Überschwemmungen und

Lebensmittelknappheit werden wahrscheinlich eine Milliarde Menschen in der Welt in Krisen stürzen, 280 Millionen Menschen von ihren Häusern vertreiben und dann entsteht ein großer Flüchtlingsstrom. Das andere ist der Konflikt zwischen Zivilisationen. Sind die Zusammenstöße zwischen Zivilisationen unvermeidlich, oder könnten die Zivilisationen in Harmonie durch Kommunikation und gegenseitiges Lernen koexistieren? Diese berühmte alte Frage steht nun wieder auf unserem Tisch, da die Welt eine immer komplexere Situation erlebt, die durch Konfrontationen zwischen Abgeschlossenheit und Öffnung und zwischen Unilateralismus und Multilateralismus gekennzeichnet ist. Dies ist eigentlich die letzte Frage für uns heute: Wohin soll die Menschheit gehen?

Am 7. Juni 2019 erklärte der UN-Generalsekretär A. Guterres im Internationalen Wirtschaftsforum Sankt Petersburg, dass „die globalen Herausforderungen globale Lösungen erfordern. Kein Land und keine Organisation kann allein mit diesen Herausforderungen zurechtkommen“. Er betonte auch, dass die Welt multilaterale Institutionen und Architektur haben muss, weil die internationalen Beziehungen auf der Basis des Völkerrechts beruhen müssen. Als weltweit größtes Entwicklungsland und ständiges Mitglied des UN-Sicherheitsrats hält sich China stets an dem Grundsatz der globalen Verwaltung, der umfassende Konsultationen, gemeinsame Beiträge und gemeinsame Vorteile beinhaltet. China hält stets an dem Weg der friedlichen Entwicklung fest, unterstützt standhaft den Multilateralismus und hält felsenfest die zentrale Rolle der Vereinten Nationen in der globalen Verwaltung aufrecht und fördert aktiv die Schaffung neuer internationalen Beziehungen und einer Schicksalsgemeinschaft der Menschheit. Es soll darauf hingewiesen werden, dass das Politische Büro des Zentralkomitees der Kommunistischen Partei Chinas eine Reihe von Studien über das Thema „globale Verwaltung“ durchgeführt hat. Präsident Xi Jinping leitete diese Sitzungen persönlich und hielt eine Reihe wichtiger Reden zu diesem Thema. Dies zeigt voll und ganz, dass China der globalen Verwaltung große Aufmerksamkeit beimisst und bereit ist, seine Rolle als ein großes und verantwortungsvolles Land in der globalen Verwaltung zu spielen, sich an der Reform und dem Aufbau des globalen Verwaltungssystems zu beteiligen und seine Weisheit und Stärke kontinuierlich zu widmen.

II

Nachdem Präsident Xi Jinping das Konzept einer „Schicksalsgemeinschaft“ der Menschheit am 23. März 2013 vorgeschlagen hatte, ist das Konzept bald zu einem „Schlagwort“ in den internationalen Beziehungen und der globalen Verwaltung geworden. Es wurde nicht nur von chinesischen Führern in verschiedenen Redebeiträgen wiederholt erwähnt und mehrmals interpretiert, sondern auch in vielen UN-Resolutionen geschrieben. Das bedeutet, dass die Schicksalsgemeinschaft der Menschheit weitgehend zu einem internationalen Konsens geworden ist. Der Bericht des 19. CPC-Nationalkongresses forderte die Menschen aller Länder auf, „gemeinsam eine Schicksalsgemeinschaft der Menschheit zu errichten, eine Welt mit dauerhaftem Frieden, allgemeiner Sicherheit, gemeinsamem Wohlstand, Offenheit und Inklusion, Sauberkeit und Schönheit zu errichten“. Auf der zweiten Plenartagung des 19. Nationalkongresses des Zentralkomitees der Kommunistischen Partei Chinas wurde erneut bekräftigt, dass das Festhalten am Weg der friedlichen Entwicklung, die Verfolgung einer für beide Seiten vorteilhaften Öffnungsstrategie und die Förderung des Aufbaus einer Schicksalsgemeinschaft der Menschheit von großer Bedeutung für die noble Sache der friedlichen Entwicklung der Menschheit sind. Auf der ersten Sitzung des 13. Nationalen Volkskongresses im März 2018 wurde der „Antrag auf Änderung der Verfassung der Volksrepublik China“ angenommen, und Förderung des Aufbaus einer Schicksalsgemeinschaft der Menschheit wurde in die Präambel der Verfassung aufgenommen, sodass dieses Konzept „Schicksalsgemeinschaft der Menschheit“ bis zur verfassungsmäßigen Ebene gesteigert und ins Rechtssystem unseres Landes aufgenommen worden ist. So wurde dieses Konzept ein wichtiger Bestandteil der Xi-Jinping-Gedanken über den Sozialismus mit chinesischen Merkmalen für eine neue Ära.

Gegenwärtig ist die globale Cyberspace-Verwaltung mit schon lange bestehenden Problemen wie unvollständigen Regeln, unangemessener Ordnung und unausgewogener Entwicklung geplagt. Gleichzeitig gibt es auch die realistische Klemme der missgestalteten Struktur, der Hegemonie und Alleinherrschaft, des Mangels an Rechtsstaatlichkeit usw.

Oberflächlich scheint es, als ob die technologischen Gemeinschaften Regeln spontan zu erstellen, in der Tat erfolgt das aber unter Kontrolle der Hegemonie und Dominanz von Ländern mit den modernsten Technologien. Und dies hat zum Machtmonopol unter dem Deckmantel von „Pseudo-Dezentralisierung“ im Cyberspace geführt. Das Internet ist keineswegs ein Ort außerhalb des Gesetzes. Die internationale Gemeinschaft braucht ein faires Rechtssystem für das Internet und erfordert gesetzliche Beratung, Anweisung, Garantie und Unterstützung seitens der internationalen Rechtsgemeinschaft. Die Idee einer internationalen Rechtsgemeinschaft spiegelt das neue Verständnis der sozialen Grundlage des Völkerrechts in China wider. Es ist von großem Wert für China in Bezug auf seine Teilnahme an der Reform des globalen Verwaltungssystems und hilft bei der Förderung des besseren Verständnisses der Beziehungen zwischen China und der Welt, verstärkt das Rederecht und Sprechfähigkeit von China in der Welt und ermöglicht China einen besseren Ansatz, wenn es mit der Welt kommuniziert, und erleichtert die Legalisierung der internationalen Beziehungen, die China immer befürwortet hat. Man kann sagen, dass es nur der einzige Weg zur Schicksalsgemeinschaft der Menschheit ist, wenn wir die Arbeit für Aufbau einer internationalen Rechtsgemeinschaft verstärken.

Das internationale Umfeld bildet die Grundlage für die Errichtung einer internationalen Rechtsgemeinschaft, während sie gesetzliche Lösungen der Probleme im internationalen Umfeld bietet. Zu den großen Problemen, mit denen die Welt konfrontiert ist, gehören immer häufigere und extremere globale Probleme, die durch die Bedrohungen von Atomkrieg, Cyber-Krieg, Finanzkrieg, biologischer Kriegsführung und nichtsoveränen Kräften, die Vielfaltigkeit und Fragmentierung internationaler Gesetze und das Fehlen an und Dezentralisierung der Bereitschaft für die globale Verwaltung verursacht werden. Es ist dringend erforderlich, dass Länder auf der ganzen Welt die Zusammenarbeit stärken und die Kommunikation vertiefen, die durch Digitalisierung, Vernetzung und intelligente Entwicklung geschaffenen Chancen gemeinsam nutzen, auf globale Herausforderungen im Bereich Recht, Sicherheit und Regierungsverwaltung gut reagieren und sich gemeinsam für eine internationale Rechtsgemeinschaft einsetzen. Die internationale Rechtsgemeinschaft erfüllt die Bedürfnisse sowohl von

China als auch von der Welt. Die internationale Rechtsgemeinschaft ist keine Vorstellung und wird bald Realität werden, solange souveräne Staaten aufgrund der Interdependenz gemeinsame Interessen haben, wegen gemeinsamer Bedrohungen gemeinsame Maßnahmen ergreifen und aufgrund des Schutzes der gemeinsamen Interessen und guten Zurechtkommens mit gemeinsamen Bedrohungen ein gemeinsames Rechtssystem aufbauen und einen gemeinsamen aber auch differenzierten Verantwortlichkeitsmechanismus für Umsetzung des gemeinsamen Rechtssystems einrichten.

III

Das Datenrechtsgesetz ist ein wichtiger Bestandteil der internationalen Rechtsgemeinschaft. Datenisierung von Allem macht einen klügeren Hintergrund, vor dem alles in der ternären Welt von Menschen, Maschinen und Dingen mit Daten ausgedrückt werden kann. Deshalb treten die Persönlichkeitsmodell-Hypothese für „Datenperson“ auf. Auf dieser Basis haben wir uns mit einer Reihe von gesetzlichen Rechten und rechtlichen Beziehungen auseinandergesetzt, die traditionelle Gesetze nicht abdecken können, wie z.B. Datenrechte, Teilhaberechte und Datenhoheit. Dazu brauchen wir neue gesetzliche Vorschriften zu formulieren, um die Dateneigentumsrechte, Datenrechte, die Datennutzung und den Datenschutz im Zeitalter der digitalen Zivilisation zu regeln. Diese neuen gesetzlichen Vorschriften bezeichnen wir als „Datenrechtsgesetz“. Unter den größten Datenphilosophen des zwanzigsten Jahrhunderts gab es zwei Hauptrepräsentanten: Kevin Kelly und Yuval Noah Harari. Die Zukunftstrilogie („*Das Ende der Kontrolle – Die biologische Wende in Wirtschaft, Technik und Gesellschaft*“; „*Was Technologie will*“ und „*das Unvermeidliche*“) von Kevin Kelly und die Kurzgeschichte-Trilogie (*Sapiens: Eine kurze Geschichte der Menschheit*; *Homo Deus: Eine kurze Geschichte von morgen*; und *21 Lektionen für das 21. Jahrhundert*) sind global groß in Mode und nahmen großen Einfluss auf die Welt. Wir bezeichnen sie als große Datenphilosophen, weil sie große Ansichten hervorbrachten. Die Kernthese hat uns gezeigt, wie das Internet die alte Welt zerschmettert.

Aber wie baut das Internet eine neue Welt auf? haben sie keine Antwort gegeben. Das Datenrechtsgesetz ist unsere rechtsstaatliche Antwort auf die diese Frage aus gesetzlicher Sicht, wie die Weltordnung erneut konstruiert werden soll.

Das Datenrechtsgesetz untersucht die „drei Trends“ im Zeitalter der digitalen Zivilisation. Der erste ist der Trend der technologischen Entwicklung. Nach der Geburt des Weltcomputers im allgemeinen Sinne des elektronischen Computers trat die Menschheit in die Ära der Informationstechnologie 1.0 ein, deren wichtige Kennzeichen die elektronische Technologie, die Computertechnologie und die Softwaretechnologie sind. Zwanzig Jahre danach führten uns der technologische Fortschritt und die Evolution des Ökosystems in die Ära der Informationstechnologie 2.0, dafür die Internet-Technologie ein wichtiges Symbol ist. Internationale Online-Plattformen wie Facebook bündeln Informationen aus der ganzen Welt, verbinden uns alle und machen unsere Welt zu einem globalen Dorf, in dem Menschen das Gefühl haben, einander nahe zu sein („das Geräusch von Huhn und Hund voneinander zu hören ist“). Dann entwickelte sich die Technologie immer weiter, was zu neuen Generationen der Technologien wie künstliche Intelligenz, Quanteninformation, 5G-Kommunikation, dem Internet der Dinge und Blockchain usw. führt. So befinden wir uns nun in der Ära der Informationstechnologie 3.0, die durch digitale Zwillinge symbolisiert wird. Die Menschheit befindet sich mitten in der Migration vom physischen Raum zum digitalen Raum. In absehbarer Zeit wird erwartet, dass sich der physische und digitale Raum beide verschmelzen. Digitalisierung, Vernetzung und Intelligenz werden allmählich zu neuen Merkmalen der menschlichen Existenz. Und das digitale Überleben wird unsere wichtigste Lebensart sein. Dies ist der „technologische Kontext“ unserer Studie über das Datenrechtsgesetz. Der zweite ist der Trend zur gesetzlichen Entwicklung. Die Entwicklung von Gesetzen ist ein Zustand der Bewusstheit der Gesellschaft. Rückblickend auf die Geschichte der Rechtssysteme der Welt sehen wir den Entwicklungsprozess von Gesetzen für ethnische Gruppen bis zu Gesetzen für Stadtstaaten, von nationalen Gesetzen bis hin zu internationalen Körperschaftsgesetzen. In Zukunft werden Gesetze von nationalen Gesetzen zu transnationalen bis zu supranationalen Gesetzen übergehen. Die wichtigsten Trends werden die Globalisierung und

Integration von Gesetzen, die Autonomie der privaten Rechte und die Verschmelzung von kodifizierten Gesetzen und präjudizialen Gesetzen etc. sein und schließlich wird eine diversifizierte Rechtslandschaft mit globalen plus nationalen Gesetzen gebildet. Das ist das „Grundurteil“, auf dem unsere Studie über das Datenrechtsgesetz basiert. Der dritte ist der große Trend der menschlichen Entwicklung. Von der Entstehung des Gesetzes bis jetzt bleiben die Rechteinhaber immer der „natürliche Mensch“. Aber vielleicht wird die menschliche Gesellschaft in naher Zukunft aus „natürlichen Menschen“, „Robotern“ und „gentechnisch bearbeiteten Menschen“ bestehen und sie drei koexistieren und zusammenleben. Wir nennen diese drei Existenzkategorien gemeinsam als „Datenperson“. Auf dieser Grundlage schaffen wir den Rechtsrahmen von „Datenrechte, Datenrechtssystem und Datenrechtsgesetz“. Dies ist die „theoretische Grundlage“ für unsere Studie über das Datenrechtsgesetz.

„Wenn die chinesischen Gesetze auf die Weltbühne gehen sollen, sind Gesetze, die mit der digitalen Wirtschaft zusammenhängen, am wahrscheinlichsten“. Die größte Veränderung in der internationalen Politik im frühen zwanzigsten Jahrhundert ist die dauerhafte und friedliche Entwicklung in China. Für jedes Land kommt der wahre Frieden aus der Versorgung der Welt mit einer Zivilisation. Das Datenrechtsgesetz bietet eine neue Ordnung, in der die Menschheit in Richtung digitaler Zivilisation marschiert. Es ist zugleich auch ein Produkt des Fortschritts unserer Zeit. Das eröffnet ein völlig neues Feld für juristische Studie und hat wichtige Bedeutung für Förderung des bidirektionalen Gesprächs zwischen dem chinesischen Rechtsbereich und dem Rechtsbereich der Welt und für Vorantreiben des Austauschs im Bereich der bilateralen und multilateralen Rechtskultur etc. Das System von „Datenrecht-Datenrechtssystem-Datenrechtsgesetz“ bietet uns einen ganz neuen Blickwinkel, damit wir diese Welt erneut genau studieren. Das ist auch ein Schlüssel, den wir alle herbeiwünschen und mit dem die künftige Tür der digitalen Zivilisation geöffnet wird. Man kann sagen, dass das Datenrechtsgesetz sowohl eine großartige Vorstellung für Studie des künftigen Lebens ist, als auch eine wichtige Entdeckung für Studie der digitalen Zivilisation darstellt. Das Angebot des Datenrechtsgesetzes hat den Grundstein dafür gelegt, die nationale Datensouveränität zu wahren, das Recht zur Erstellung der

Datenregel und das internationale Rederecht fest in der Hand zu nehmen sowie die rechtstaatliche globale Verwaltung zu fördern. Das hat für die Beförderung des Aufbaus einer Schicksalsgemeinschaft der Menschheit auch besondere Bedeutung.

Datenperson

Das Recht ist eng mit der menschlichen Natur verbunden. „Die menschliche Natur ist die Quelle und Grundlage des Rechts. Das Recht stellt wiederum die Anforderung und Verkörperung der menschlichen Natur dar. Die auf der menschlichen Natur beruhenden Rechte sind tief verwurzelt. Das Ausmaß, in dem man die menschliche Natur versteht, bestimmt also, in welchem Maße Menschen ihre Rechte verstehen und dann in solchem Maße in der Lage sind, Rechte schützen zu können“. Das Gesetz ist ein Regelsystem, das auf der Basis der Forderung der menschlichen Natur entstanden hat. Das ist die äußere Ausdrucksform der menschlichen Forderung nach Regeln. Es beginnt und endet all mit dem Menschen. Das Gesetz entspringt der menschlichen Natur. Und das Studium des Rechts verliert seine theoretische Prämisse, wenn es sich von der menschlichen Natur trennt. „Was wir brauchen, ist Interpretierung des Wesens des Gesetzes. Und dieses Wesen soll aus der menschlichen Natur gefunden werden“. Die menschliche Natur ist die Grundlage für die Beurteilung der Rechtmäßigkeit des Gesetzes und der Strukturierung des Rechtssystems. Wir treten jetzt in eine neue Ära der Zivilisation ein, die durch die Struktur der digitalen Wirtschaft, digitalen Regierung und digitalen Gesellschaft gekennzeichnet ist. Die Schaffung einer digitalen Zivilisation stützt sich auf die Gestaltung von Regeln für Datenrechte, die Ausgestaltung eines Systems für Datenrechte und die Festlegung des Datenrechtsgesetzes. Als solche wird die Gesetzgebung über Datenrechte zu einem unvermeidlichen Trend der Entwicklung der menschlichen Gesellschaft. Für die Studie über das Datenrechtsgesetz e ist die Hypothese der menschlichen Natur der logische Ausgangspunkt und der Kern des Werts. Wir schlagen die menschliche Natur des Datenrechts als Datenperson-Hypothese vor und der

Kern dieser Hypothese ist Altruismus. Eben deshalb der Altruismus möglich ist, können Ansprüche auf Datenrechte möglich werden.

Abschnitt I Menschliche Basis des Gesetzes

Alle Doktrinen über den Menschen haben die bestimmte Hypothese der menschlichen Natur als ihre Prämisse und Ausgangspunkt genommen. Die verschiedenen Definitionen des Menschen und verschiedene Hypothesen der menschlichen Natur bestimmten die Grundneigung der verschiedenen Disziplinen. Wie David Hume sagte: „Alle Wissenschaften haben mehr oder weniger ein Verhältnis zur menschlichen Natur und dass sie immer noch um eine oder andere Passage zur menschlichen Natur zurückkehren, wie weit sie auch immer von ihr zu laufen scheinen“ (David Hume 1996, S. 6). Jedes Systemdesign hat eine gewisse Hypothese der menschlichen Natur als seine Prämisse angedeutet. „Die verschiedenen Systeme basieren auf ihren unterschiedlichen hypothetischen Möglichkeiten der menschlichen Natur, sie organisieren, leiten, kontrollieren und stimulieren Menschen auf verschiedenartige Weise“ (Gao Chengjun 2014). Was den Aufbau eines beliebigen institutionellen Systems betrifft, so kann es nur dann eine theoretische Abstraktion vermeiden, wenn der logische Ausgangspunkt klargestellt ist. Wie Yi-Hwa Yang, ein Gelehrter aus Taiwan von China, einmal zu dieser Frage kommentierte, „ist die Jurisprudenz ein Thema des menschenorientierten Rechtsstudiums. Die Studie über die Jurisprudenz muss sich auf die Studie über die menschliche Mentalität konzentrieren; die Rechtsgrundsätze sind schließlich untrennbar mit dem Menschen an sich, der menschlichen Wechselwirkung und den sozialen Szenarien, in denen der Mensch um seine Existenz kämpft“ (Hu Yuhong 2002, S. 7). „Die Rechtswissenschaft ist eine Wissenschaft des Menschen. Sie ist eine menschenorientierte Wissenschaft. Sie konzentriert sich auf das tatsächliche rechtliche Leben der Menschen und die rechtlichen Fragen, denen sich die Menschen im sozialen Leben gegenübersehen. Die sogenannten „rechtlichen Phänomenen“ sind nichts anderes als verschiedene Verhaltensphänomene, die von Menschen

in rechtlichen Szenarien dargestellt werden. Zu viel Legung des Nachdrucks auf rechtliche Phänomene, die das Objekt der Rechtsstudie sind, könnte dazu führen, dass man vergisst, wer solche Phänomene verursacht hat und es unmöglich machen, die inhärente Spannung zwischen Mensch und Recht zu untersuchen, die sich aus rechtlichen Fragen ergibt“ (Hu Yuhong 2002, S. 6).

(I) Mensch und menschliche Natur

Die vorausgesetzte Hypothese aller Humanwissenschaften konzentriert sich auf die Menschenzentrierung und die Aufmerksamkeit für die menschliche Natur. Bereits im antiken Griechenland versuchten die Weisen, das „Rätsel von Sphinx“ der menschlichen Natur zu lösen. Im Mittelalter handelte die Gründung der Weltsicht der Menschen von der Theologie und die Göttlichkeit wurde benutzt, um die menschliche Natur zu gestalten und diese zu erklären. Erst in der Zeit der Renaissance wurde der Mensch auf den menschlichen Körper, Geist, Wunsch und Wohlbefinden im Rampenlicht aufmerksam. Dies wurde in der Geschichtswissenschaft als „Entdeckung des Menschen“ genannt. Aber was ist der Mensch? Das war seit der Antike der in- und ausländischen Gedankengeschichte immer eine viel geredete Frage für Philosophen auf der ganzen Welt. Es ist auch ein faszinierendes und seit jeher bestehendes Thema. Wie ein Schatz, der niemals ausgetrocknet und voller Versuchung ist, zieht es zahlreiche antike und moderne chinesische und ausländische Philosophen an, darüber Gedanken zu machen und von ihm gequält zu werden. Die Debatten darüber haben im vergangenen Jahrtausend nie aufgehört.

Viele Philosophen, chinesische und ausländische, alte und moderne, haben ihre Ansichten über die menschliche Natur zum Ausdruck gebracht und zahlreiche literarische Schriften zu diesem Thema in der Geschichte wurden hinterlassen. Trotzdem scheint es jedoch kein Anzeichen für einen Konsens zu geben. Bis zurzeit ist immer noch kein Zeichen für einen Konsens sichtbar. Dies könnte einer der Gründe sein, warum dieses Thema immer so weit verbreitet und darüber viel diskutiert wurde. Hier

sind einige der Ansichten: Protagoras sagte: „Der Mensch ist das Maß von allen Dingen“. Aristoteles sagte: „Der Mensch von Natur aus ist ein politisches Tier“. Ein Motto im Mittelalter lautet: „die Hälfte des Menschen ist Engel und die andere Hälfte ist Tier“. La Mettrie sagte: „Mensch ist Maschine“. Immanuel Kant sagte: „Mensch ist Ziel“. Utilitaristen sagten: „Mensch ist ein rationaler Maximierender seiner Interessen“. Karl Marx sagte: „Der Mensch ist die Summe der sozialen Beziehungen“. Ernst Cassirer sagte: „Der Mensch ist ein kulturelles Tier oder ein Tier, das Symbol verwendet“. Friedrich Nietzsche sagte: „Der Mensch ist das Tier des Willens der Macht“. Pascal sagte: „Der Mensch ist ein denkendes Schilf“. Und Mark Twain sagte einmal: „Der Mensch ist das einzige Tier, das Scham weiß oder sich zu beschämen braucht“ und so weiter. All diese Theorien liefern sehr richtige Antworten auf die menschliche Natur aus verschiedenen Perspektiven, aber sie sind noch wahrscheinlicher „nur ein Glied in der Kette der ewigen Entwicklung, in der die Menschheit in ihr eigenes Mysterium ergründet“ (Chen Zhonglin 2001). Keiner von ihnen bekommt alles.

Tabelle 1-1 Alte und moderne sowie chinesische und ausländische Definitionen des „Menschen“

Definition	Quelle
Der Mensch ist eine Schöpfung Gottes.	Kommt vor allem aus frühen Mythen und christlicher Theologie. Nach der in der christlichen Bibel angegebenen Schöpfungslehre schuf Gott die Himmel und die Erde und schuf am sechsten Tag der Erschaffung der Welt den Menschen nach seinem eigenen Bild und ließ den Menschen über jedes Lebewesen herrschen, das sich auf der Erde bewegt.
Der Mensch ist ein rationales Tier.	Mit der längsten Geschichte ist diese Idee die einflussreichste und heute noch weit verbreitet. Sokrates definiert den Menschen als Kreatur, die eine rationale Antwort auf rationale Frage geben kann. Xunzi sagte, dass der Mensch deshalb ein Mensch ist, warum? Weil er Unterscheidungen hat, nicht deshalb, nur weil er zwei Beine und keine Federn hat.

Tabelle 1-1 Fortsetzung

Definition	Quelle
Der Mensch ist ein politisches Tier.	Wurde zuerst von Aristoteles vorgeschlagen. Nach seinem Dafürhalten wird allen Menschen von Natur aus ein sozialer Instinkt eingepflanzt und kann so unerwartet eine solche fortschrittliche (politische) Allianz bilden. Deshalb ist der Mensch von Natur aus ein politisches Tier. Wie Xunzi sagte, ist er nicht so stark wie ein Ochse, noch so schnell wie ein Pferd, und doch lässt er den Ochsen und das Pferd für ihn arbeiten. Warum? Weil er in der Lage ist, sich in der Gesellschaft zu organisieren und sie nicht.
Der Mensch ist ein sprachliches Tier	Aristoteles erklärte, der Mensch sei das einzige Tier, das in der Lage ist, sich in Sprache auszudrücken. Martin Heidegger sagte, die Sprache sei die Heimat des Daseins. Cassirer sagte, der Mensch sollte als ein symbolisches Tier definiert werden. Obwohl die moderne Beobachtung und Untersuchung von Tieren bewiesen hat, dass Tiere auch ihre Sprachen haben und in der Lage sind, Informationen mit ihren Gegenstellen zu tauschen und zu teilen, gibt es zeitgenössische Anthropologen, die immer noch darauf bestehen, dass der Mensch das einzige Wesen ist, das sprachliche Zeichen zur Kommunikation verwenden kann.
Der Mensch ist ein moralisches Tier	Mencius sagte: der Mensch (im Gegensatz zu den unteren Tieren) sei nur klein. Die Masse der Menschen wirft es weg, während überlegene Männer es bewahren. Shun verstand die Vielfältigkeit der Dinge klar und beobachtete die Beziehungen der Menschheit. Er ging auf dem Weg des Wohlwollens und der Gerechtigkeit; er brauchte nicht nach Wohlwollen und Gerechtigkeit zu streben. Xunzi sagte, Feuer und Wasser besitzen Energie, aber sie sind ohne Leben. Gras und Bäume haben Leben, aber keine Intelligenz. Vögel und Tiere haben Intelligenz, aber keinen Sinn für Pflicht. Nur der Mensch besitzt Energie, Leben, Intelligenz und zusätzlich das Pflichtgefühl. Deshalb ist er das edelste Wesen auf der Erde. Zhu Xi sagte, dass der Mensch anders sei als die Tiere, da es Liebe zwischen Vater und Sohn gebe; Gerechtigkeit zwischen einem Herrscher und Diener; Trennung von Funktionen und Jobs zwischen einem Mann und einer Frau, wie sie alle ihren Platz und angemessene Verantwortlichkeiten kennen sollten; eine ordentliche Ordnung zwischen Alt und Jung und Treue zwischen Freunden.

(Fortsetzung)

Tabelle I-1 Fortsetzung

Definition	Quelle
Der Mensch ist ein Werkzeug-Tier	Benjamin Franklin definierte den Menschen als ein „Werkzeugmachendes Tier“; Friedrich Engels definierte den Menschen als „Tiere, die Werkzeuge herstellen und verwenden“; Anthropologen George Bartholomew Jr. und Joseph Birdsell sagten, dass das einzige Säugetier ist, das ständig mit Werkzeugen für das Überleben sorgen kann; der chinesische Philosoph Deng Xiaomang sagte, der Mensch sei ein Tier, das Werkzeuge herstellt, verwendet und befördert.
Der Mensch ist ein spirituelles Tier	Georg Wilhelm Friedrich Hegel definierte den Menschen als selbstbewusstes Tier; Ludwig Feuerbach definierte den Menschen als ein Tier mit ideologischen Gefühlen; Wilhelm Dilthen erneuerte die spirituelle Kultur als Unterscheidung zwischen Mensch und Tier; Max Scheler definierte den Menschen als das einzige überlegene Dasein mit geistiger Tendenz; Erich Rothacker war der Meinung, dass das Wesen des Menschen in seiner geistigen Tätigkeit lag; Michael Landmann sagte, der Mensch sei eine spirituelle Kreatur.
Der Mensch ist ein kulturelles Tier	Ernst Cassirer definierte den Menschen als ein Tier der Kultur; Michael Landmann betrachtete den Menschen als das, was die Kultur erschafft und anwendet; Shi Zhonglian deutete die Kultur als alles, was der Mensch erschaffen hat, und sagte, dass ein wirkliches und tiefgründiges Verständnis des besonderen Eigentums des Menschen nur erlangt werden könne, wenn der Mensch als Wesen der Kultur angesehen würde.
Der Mensch ist eine unspezialisierte Schöpfung	Arnold Gehlen erklärte, der größte Unterschied zwischen Mensch und Tier sei, dass der Mensch unspezialisiert sei. Da er unspezialisiert oder nicht bestimmt war, konnte der Mensch seine Funktionsmängel wettmachen, sich mit ausreichend ausgerüsteten Tieren auszeichnen und der Welt gegenüber offen sein, ohne von der Umgebung eingeschlossen zu werden. Dies war die Art, wie der Mensch alle Defekte in der Struktur der Kreatur lösen konnte.

Tabelle 1-1 Fortsetzung

Definition	Quelle
Der Mensch ist ein freies Tier	Die Befürworter dieser Definition sind unter anderem Chuang Tsi aus dem alten China und eine große Anzahl jüngerer Denker seit der Aufklärung: Jean-Jacques Rousseau, Immanuel Kant, Karl Marx und Jean-Paul Sartre usw. Karl Marx ist vielleicht der repräsentativste. Seine Definition des Menschen könnte durch die Schlussfolgerung sein, dass der Mensch ein freies und bewusstes Tier sei. Diese Definition hinderte ihn keineswegs daran, in seinem Alter Benjamin Franklin die Definition des Menschen zu bekräftigen, da die Herstellung von Werkzeugen genau eine Art freier und bewusster Aktivität ist.

Quelle: Han Dongping. „Das Geheimnis des Menschen lösen: Dekonstruktion und Rekonstruktion der Definition des Menschen, Wuhan Universität Journal (Geisteswissenschaften), sechste Ausgabe 2016

Natürlich gibt es kein Ende unserer Bemühungen, den Menschen zu definieren, und neue Definitionen werden nacheinander auftauchen. Die Definition des Menschen muss dekonstruiert und rekonstruiert werden. Die Diskussion darüber, was der Mensch ist, ist deshalb notwendig, weil das menschliche Leben eine Realität ist, die von einem institutionellen Rahmen beherrscht wird. Karl Marx zeigte die wesentliche Eigenschaft des „Menschen“ aus drei Perspektiven. Er offenbarte die Unterscheidung zwischen Mensch und Tier aus der Perspektive der Arbeit, erklärte die Beziehungen zwischen Personen aus der Perspektive der Geselligkeit und präziserte aus der Perspektive der Entwicklung des Menschen an sich, dass die eigene Nachfrage des Menschen selbst das Wesen des Menschen war (Yang Lan 2018). Die Komplexität des Menschen bestimmt, dass die menschliche Natur multidimensional ist. Anders als Göttlichkeit und Animalität ist die „menschliche Natur der Oberbegriff verschiedener Attribute des Menschen“ im Allgemeinen. Sie beinhaltet vor allem die natürliche, soziale und spirituelle Eigenschaft. Und in dialektischer Einheit bilden die drei die vollständige Struktur der menschlichen Natur. Wie durch Produktionsbeziehungen, politische und ethische Beziehungen usw. eingeschränkt,

verändert sich die menschliche Natur unter anderem ständig im Prozess der sozialen Entwicklung.

Unter der natürlichen Eigenschaft des Menschen wird eine Summe von Charakterszenarien des Menschen verstanden, der als natürliches Wesen der Natur unterliegt. Wie jede andere Lebensform ist der Mensch auch ein Ergebnis der Entwicklung nach der natürlichen Regelmäßigkeit und macht physikalische und chemische Bewegungen. So hat der Mensch die Eigenschaften der Dinge. Als eine Art von Tier führt der Mensch als Lebewesen Tätigkeiten durch und hat die Eigenschaften, die die Tiere im Allgemeinen besitzen. Der natürliche Aspekt und die sich daraus ergebenden Wünsche des Menschen bilden die materielle Basis für die Existenz des Menschen und dienen als Vorbedingungen für alle menschlichen Tätigkeiten und andere Eigenschaften der menschlichen Natur. Wie Friedrich Engels sagte: „Es ist jedoch inhärent in der Abstammung des Menschen aus der Tierwelt, dass er sich niemals vollständig von dem Tier befreien kann, sodass es immer nur eine Frage von mehr oder weniger Freiheit davon sein kann, eines Unterschieds im Grad der Bestialität oder der Menschlichkeit“. „Der Mensch ist unmittelbar ein natürliches Wesen. Als natürliches Wesen und als lebendiges natürliches Dasein ist er einerseits mit natürlichen und vitalen Kräften ausgestattet und gilt als aktives natürliches Wesen. Diese Kräfte existieren in ihm als angeborene Gabe und Fähigkeit und als Verlangen“ (Das zentrale Kompilations- und Übersetzungsbüro 2009, S. 209). „Die Menschlichkeit ist Natur des Menschen“ (Das zentrale Kompilations- und Übersetzungsbüro 2009, S. 208). Der Mensch ist vor allem ein natürliches Wesen und dann ein soziales Wesen, rationales Wesen, kulturelles und ethisches Wesen.

Das soziale Attribut des Menschen ist die Gesamtheit aller Eigenschaften des Menschen als soziales Wesen. Anders als andere Tiere in der Handlungsart und -weise, lebt der Mensch in sozialen Gruppen, deshalb bekommt der Mensch eine neue Eigenschaft – Sozialität. Laut Ludwig Feuerbach ist nur der soziale Mensch ein Mensch (Ludwig Feuerbach 1984, S. 571). Karl Marx war der Meinung, dass der Mensch sowohl von Natürlichkeit als auch von Geselligkeit ist und dass der Mensch nur in den sozialen Beziehungen ein Mensch sein kann. Er definierte das Wesen des Menschen „nicht als abstraktes Ding, die jedem

einzelnen Individuum innewohnt; in seiner Realität ist er das Ensemble aller sozialen Beziehungen“. Je weiter wir den Verlauf der Geschichte zurückverfolgen, desto mehr wirkte das Individuum, und damit auch das produzierende Individuum, abhängig und zu einem größeren Ganzen zu gehören: Zuerst ist das Individuum noch ganz natürlich ein Teil der Familie und des Stammes, der sich aus der Familie entwickelt; später ist er Teil einer Kommune, einer der verschiedenen Formen der Gemeinschaft, die aus dem Konflikt und der Verschmelzung der Sippen entstand. Erst im achtzehnten Jahrhundert spiegelten die verschiedenen Formen der sozialen Beziehungen in der bürgerlichen Gesellschaft für das Individuum in der äußeren Unvermeidbarkeit wider. Aber die Epoche, in der dieser Standpunkt, nämlich der des isolierten Individuums, hervorgerufen worden ist, ist gerade die Epoche der bisher höchst entwickelten sozialen Beziehungen. Der Mensch ist ein politisches Tier im wahrsten Sinne des Wortes, nicht nur ein geselliges Tier, sondern ein Tier, das nur innerhalb der Gesellschaft individualisiert werden kann. Die Produktion durch eine isolierte Person außerhalb der Gesellschaft ... ist unvorstellbar (Karl Marx 1979, S. 22).

Die natürlichen und sozialen Eigenschaften sind nur der Ausgangspunkt der menschlichen Natur und keineswegs das Ganze der menschlichen Natur. Wichtiger ist, dass der Mensch auch noch die moralischen Eigenschaften besitzt. Diese Eigenschaften ergeben sich aus der Tendenz des Menschen, dass er im Umgang mit anderen Menschen oder mit der Gesellschaft Maßnahmen ergreift, die auf spezifischen Verhaltenskodizes beruhen. Die Moralität ist die einzigartige Eigenschaft der menschlichen Natur, die den Menschen von anderen Tieren unterscheidet und den Menschen anderen Tieren überlegen macht. In Bezug auf Moral und Ethik unterscheidet die moralische Natur des Menschen durchaus nicht nur von den Tieren in ihrem Inhalt, sondern auch in ihrer Form. Im Kapitel über Regeln eines Königs sagte Xunzi: „Feuer und Wasser besitzen Energie, aber sie sind ohne Leben. Gras und Bäume haben Leben, aber keine Intelligenz. Vögel und Tiere haben Intelligenz, aber keinen Sinn für Pflicht. Der Mensch besitzt aber Energie, Leben, Intelligenz und zusätzlich auch das Pflichtgefühl. Deshalb ist er das edelste Wesen auf der Erde“. Das heißt, der Mensch ist deshalb den Vögeln und Tieren im Allgemeinen überlegen,

weil der Mensch über Gut und Böse Bescheid weiß und das moralische Gefühl hat. „Das wichtigste in diesem Merkmal ist vor allem der Altruismus. Das heißt, der Mensch zeigt Respekt und Fürsorge gegenüber anderen Menschen, die in derselben Gruppe leben, schenken der Gruppe und sogar der ganzen Menschheit und der Natur Aufmerksamkeit, und lässt seine Handlungen in Einklang mit der Umgebung stehen und anderen zugutekommen und die Entwicklung der Gruppe, in der sie leben fördern“ (Yan Cunsheng 2007). Die moralische Natur ist eine überragende Natur, die auf Rationalität, Sensibilität und Gesellschaftlichkeit beruht und die organische Kombination der drei bildet. Die wesentliche Eigenschaft ist Altruismus und Zivilisation.

(II) Einige Hypothesen der menschlichen Natur

Die Hypothesen der menschlichen Natur sind Annahmen der wesentlichen Natur des Menschen. Die menschliche Natur ist der Ort, an dem wir Antworten auf Fragen finden können, die sich auf die Beziehungen zwischen Mensch und Natur, Mensch und Gesellschaft sowie auf den Menschen selbst beziehen. Darüber hinaus sind Hypothesen der menschlichen Natur immer der logische Ausgangspunkt unserer Studien über Themen, die unter anderem Verwaltungsaktivität, institutionelle Gestaltung, Innovation in Regeln und gesetzliche Vorschriften usw. in der Realität betreffen, weil all dies die Hypothesen der menschlichen Natur auf die eine oder andere Weise darstellt. Es gab in der Gedanken- geschichte der Menschlichkeit unzählige Theorien über die Hypothesen der menschlichen Natur, aber es sind nur diejenigen Hypothesen der menschlichen Natur in einigen spezifischen Disziplinen, die in der Realität wirklich einflussreich sind und ihre Anwendungen weit verbreitet sind (siehe Tabelle 1-2).

Tabelle 1-2 Einige klassischen Hypothesen der menschlichen Natur

Hypothese	Beschreibung
Hypothese des Wirtschaftsmenschen	Der Gedanke des „Wirtschaftsmenschen“ wurde zuerst von Adam Smith in <i>The Wealth of Nations</i> vorgebracht. Der Kern dieser Idee ist, dass der Zweck der menschlichen Aktivitäten ist, die Vorteile des Menschen zu maximieren. Diese Hypothese hat einen tief greifenden Einfluss auf die industrielle Gesellschaft und bildet die Grundlage für Strukturierung der Gesellschaft und der institutionellen Strukturen im Westen. In der Zwischenzeit haben die Menschen in dieser Ordnung eine „unsichtbare Hand“ gefunden, die unbewusst aber auch effektiv die sozialen und öffentlichen Interessen verstärken kann, während die Individuen die Maximierung ihrer eigenen Interessen verfolgen. Diese Hypothese und relevante Gedanken haben zur Entstehung der wissenschaftlichen Managementtheorie beigetragen.
Hypothese des politischen Menschen	In der „Politik“ stellte Aristoteles die Idee vor, dass der Mensch von Natur aus ein politisches Tier im Bereich der Gewaltenteilung ist. Nach dieser Hypothese ist der Mensch eine Art Tier, das in der Lage ist, Interessen anzupassen und guten Willen und Zusammenarbeit zu verfolgen und immer dazu neigt, politische Gemeinschaften zu bilden. Die Bürger eines Stadtstaates wurden gleichberechtigt geschaffen und nach dem Prinzip der Fairness und Gerechtigkeit direkt an staatlichen Angelegenheiten beteiligen und diese verwalten. Die Hypothese des politischen Menschen zeigt die Untrennbarkeit von Mensch und Politik in einer Klassengesellschaft, in der soziale Interessen sehr differenziert sind. Sie hat einen positiven Beitrag zur Lösung des Mysteriums der menschlichen Natur geleistet. Die seit langem bestehende Theorie der Menschenrechte in westlichen Ländern ist genau von Aristoteles Theorie über politischen Menschen abgeleitet.

(Fortsetzung)

Tabelle 1-2 Fortsetzung

Hypothese	Beschreibung
Hypothese des moralischen Menschen	<p>Im Buch "Theorie des moralischen Sentiments" hielt Adam Smith fest, dass jeder Mensch moralischen Sinn hat und ein präziser Ausdruck davon ist, dass die Menschen Mitgefühl und Gerechtigkeit haben. Das Verhalten von Menschen zeigt eine altruistische Tendenz und verfolgt die Maximierung von kollektiven Interessen. Die von Adam Smith vorgelegte Doktrin des moralischen Menschen hat viel mit der Doktrin der guten menschlichen Natur zu tun, die Mencius in der Prä-Qin-Zeit im alten China geschrieben hat. In der traditionellen chinesischen Gesellschaft war der moralische Mensch als menschliche Grundlage für das Top-Level-Design und institutionelle Anordnungen der Gesellschaft und die Hypothese des moralischen Menschen hatte ihren eindeutigen Einfluss auf die traditionelle chinesische Gesellschaft.</p>
Hypothese des Sozialmenschen	<p>Basierend auf den Hawthorne-Experimenten gründete Professor Elton Mayo von der Harvard University, ein Managementwissenschaftler, die Theorie über Human Relations School und schlug offiziell die systematische Hypothese des sozialen Menschen im Buch „The Human Problems of a Industrial Civilization“ vor. Er vertrat die Auffassung, dass ein sozialer Mensch ein Mensch ist, der sich in verschiedenen sozialen Beziehungen befindet und unterschiedliche soziale Forderungen hat. Er hat nicht nur das Motiv, persönliche Vergütung und Einkommen zu verfolgen, sondern auch die Forderungen nach Freundschaft, Sicherheitsgefühl und Mitgliedschaft usw. Die Hypothese des sozialen Menschen betont, dass menschliche Beziehungen und die Mitgliedschaft in Organisationen bei der Stimulierung des menschlichen Verhaltens wirksamer sind als finanzielle Kompensation. Die Umwandlung von der Hypothese des Wirtschaftsmenschen in die Hypothese des sozialen Menschen ist zweifellos ein großer Fortschritt in den Managementgedanken und der Managementmethode.</p>

Tabelle 1-2 Fortsetzung

Hypothese	Beschreibung
Hypothese des Kulturmenschen	In seinem Meisterwerk „An Essay on Man“ legte Ernst Cassirer, ein deutscher Philosoph und Gründer der Kulturphilosophie, die Idee des „Kulturmenschen“ vor. 1981 veröffentlichte William Ouchi, Professor an der UCLA, „Theory Z: How American Business Can Meet the Japanese Challenge“, die bahnbrechende Arbeit an der Theorie der Unternehmenskultur. In diesem Buch stellte er die Hypothese des Kulturmenschen dar und vertrat die Ansicht, dass Psychologie und Verhalten des Menschen letztendlich von kulturellen Faktoren wie Wertanschauung usw. bestimmt werden. Die Kulturmensch-Hypothese offenbart die kulturelle Natur, eine zugrunde liegende Natur des Menschen, greift tiefer in die menschliche Natur ein und hat einen tief greifenden Einfluss in der Realität.

Die oben genannten Theorien über die menschliche Natur enthüllen offensichtlich einen einseitigen Aspekt der menschlichen Natur. Die Hypothese des Wirtschaftsmenschen zeigt zum Beispiel den Egoismus des Menschen; die Hypothese des politischen Menschen hebt die soziale Natur des Menschen hervor; in der Hypothese des moralischen Menschen steht der Altruismus der menschlichen Natur vor; die Hypothese des Sozialmenschen überragt die nichtwirtschaftliche Gesellschaflichkeit des Menschen, während die Hypothese des Kulturmenschen die kulturelle Einbettbarkeit des Menschen markiert. Obwohl es Rechtfertigungen für ihre Existenz gibt, ziehen diese Hypothesen der menschlichen Natur Schlussfolgerungen auf der Grundlage einer Überverallgemeinerung bestimmter Verhaltensweisen des Menschen und sind in der Theorie unvermeidlich partiell und in der Praxis irreführend. Infolgedessen werden sie selten angewandt. Diese Hypothesen der menschlichen Natur haben auf die Gesellschaft großen positiven Einfluss und gleichzeitig auch gewisse negative Auswirkungen geübt. Daher ist eine reflexive Überlegung notwendig, während ihnen Anerkennung gewährt wird.

(III) Menschlichkeitshypothese des Gesetzes

Der Mensch ist der logische Ausgangspunkt der Entstehung der sozialen Regeln. Und die Menschlichkeit liegt im Kern und dient als Seele beim Aufbau sozialer Regeln. Jede institutionelle Gestaltung hat ein tiefes Denken über die menschliche Natur, die dahinter liegt. In jedem Zeitalter basieren das Gesetz und die Rechtsstaatlichkeit auf der Bewertung der menschlichen Natur, während unterschiedliche Bewertungen zu unterschiedlichen Methoden der sozialen Kontrolle führen. Nur diejenigen Gesetze, die den menschlichen Anforderungen entsprechen, würden von den Menschen eingehalten, während diejenigen, die von der Menschlichkeit abweichen, nur ein Stück Papierfetzen sein könnten. Die Rechtfertigung von Gesetzen an sich liegt zu einem ziemlich großen Teil darin, ob sie mit der menschlichen Natur in Einklang stehen. Deshalb müssen wir in der menschlichen Natur Begründungen für die Notwendigkeit und Unvermeidlichkeit der Gesetzgebung zu Datenrecht finden. Wie Oliver Wendell Holmes Jr. einmal sagte, fand das Gesetz seine Philosophie aus den Bedürfnissen der menschlichen Natur (Bernard Schwatz 1989, S. 134). Ohne der menschlichen Natur Bedeutung beizumessen, kann die analytische Rechtskunde die Höhe der Rechtsphilosophie nicht erreichen. In der heute „auf Menschen ausgerichteten“ Welt ist es umso wichtiger, dass wir die menschliche Natur als Maßstab für Verdienste und Fehler des Gesetzes nutzen. Ein sogenanntes „gutes Gesetz“ sollte in der menschlichen Natur begründet sein, und die Wertansicht, die es verfolgt, und die von ihm erzeugte Rechtsordnung sollten sowohl der menschlichen Natur entsprechen als auch zum Überleben und zur Entwicklung der Menschheit beitragen.

Die bestehenden moralischen Prinzipien und Gesetze sind auf der Grundlage der menschlichen Natur festgelegt. Die „Hypothese des Wirtschaftsmenschen ist die menschliche Basis des Zivilrechts. Das Zivilrecht hat gerade diese als Prämisse für Regulierung des Verhaltens der Sozialaktivisten der Bürger und Festlegung entsprechender Vorschriften genommen“ (Yi Jun 2006). Philosophen und Denker, darunter Mencius

und Xunzi im alten China und Plato und Aristoteles im antiken Griechenland sowie Thomas Hobbes und Jean-Jacques Rousseau in der modernen Zeit usw. haben alle ihre einzigartigen und tief gehenden Einsichten in die Beziehungen zwischen den Gesetzen und der menschlichen Natur (siehe Tabelle 1-3 und 1-4) angeboten. Das Verständnis der menschlichen Natur ist der Schlüssel zum Verständnis des Menschen. Einige nehmen die menschliche Natur aus der Perspektive des natürlichen Aspekts des Menschen wahr; einige nähern sich der Menschlichkeit aus der Perspektive der Sozialität des Menschen; einige betrachten die menschliche Natur aus der Perspektive der Ethik, während die anderen die Menschlichkeit aus der Perspektive der Klasse analysieren ... und so haben sie unterschiedliche Schlussfolgerungen für die menschliche Natur gezogen. Unterschiedliche Theorien über Menschlichkeit führen unweigerlich zu unterschiedlichen Ansichten über das Gesetz, während unterschiedliche Ansichten über das Gesetz verschiedene Theorien über Menschlichkeit widerspiegeln. „Das Gesetz ist eine Kreation der Menschen und deswegen ist es auf die eine oder andere Weise mit der Menschlichkeit zwangsläufig verbunden. Das Gesetz ist einfach ein Produkt der Entwicklung der Menschlichkeit“ (Zhuo Zeyuan 2001, S. 85). Was an dem Stil eines juristischen Zeitalters wichtig ist, ist nichts anderes als seine Ansicht zu Menschen, die die Richtung des Gesetzes bestimmt (Gustav Radbruch 2001, S. 141). Unter verschiedenen historischen Bedingungen ist die Menschlichkeitshypothese des Gesetzes auch unterschiedlich und verschiedene Menschlichkeitshypothesen führen zu unterschiedlichen Merkmalen des Gesetzes in verschiedenen Stadien.

Tabelle 1-3 Gedanken über die Grundlagen der Menschennatur im alten China

Repräsent. Figur	Grundlegende Idee
Xun Kuang	Das Gesetz ist eine Ableitung von Riten und Gerechtigkeit (li und yi); es ist für eine Reihe von Sozialsystemen entwickelt, um eine ordnungsgemäße Umsetzung der beiden in der Verhaltensweise der Menschen zu gewährleisten.
Guan Zhong, Wang Chong, LüWen und Bai Juyi	Das Gesetz ist ein Derivat moralischer Prinzipien und ein Hilfsmittel zur Realisierung moralischer Regeln und Riten. Sie sind im Allgemeinen aber der Ansicht, dass das Gesetz, obwohl es offensichtlich notwendig ist, aber nicht zu viel sein sollte, oder wenn es zu viel wäre, würde mehr Schaden als Nutzen angebracht. Sie befürworteten die „Vereinbarkeit von Rechts- und Verwaltungsvorschriften“ im Bereich des öffentlichen Auftragswesens.
Guan Zhong und Xun Kuang	Das Gesetz hat eine enge Beziehung zu seinem Schöpfer und ist sowohl Produkt als auch Ausdruck der menschlichen Natur seines Schöpfers. Der Monarch und die Weisen sollten die Urheber des Gesetzes sein, weil ihre menschliche Natur gut und unmittelbar in Einklang mit der natürlichen Gerechtigkeit steht. Deshalb sind sie das Modell und Verteidiger der moralischen Prinzipien im Land und in der Lage, eine Reihe von detaillierten Riten und Gesetzen nach moralischen Grundsätzen zu geben.
Konfuzius	Die menschliche Natur ist der moralische Charakter des Menschen. Sein Kern ist die wohlwollende Natur des Menschen. Das heißt, wohlwollende Menschen haben fürsorgliche und liebevolle Herzen und Menschen an der Macht adoptieren wohlwollende politische Strategie, und das Gesetz ist so eine Maßnahme für Verwendung von obligatorischen Mitteln, um wohlwollende Regel auf der Basis dieser Notwendigkeit umzusetzen.

Quelle: Yan Chunsheng: „Rechtsgrundlage aus Sicht der menschlichen Natur“, Verlag des chinesischen Rechtssystems, 2016

Das Verständnis der Dinge ist durch Veränderung des Zeitalters und kulturelle Diskrepanz auch unterschiedlich. Allerdings ist dieser Unterschied meist nur in Worten, während es in Bezug auf grundlegende Konnotation oder Blickwinkel der Studie sehr ähnlich ist. Dies gilt insbesondere für Studien über das Thema „menschliche Natur des Gesetzes“ in der chinesischen und ausländischen Geschichte. In ihren Diskussionen über die Zusammensetzung der menschlichen Natur und die Beziehungen zwischen den verschiedenen Elementen betrachteten sowohl chinesische als auch ausländische Gelehrte den Menschen als eine Kombination von Rationalität und Sensibilität. Die Erstere macht den Menschen virtuell, während die Letztere den Menschen dazu bringen, böse Dinge zu tun. Sie alle betrachteten die menschliche Natur in einigen Dimensionen, d.h. die geborene natürliche Eigenschaft und die erworbene soziale Natur. Obwohl sie im Grunde die gleiche Wahrnehmung des Gesetzes hatten und das Gesetz als Regel und Verwaltungsinstrument in der Gesellschaft ansahen, hatten sie aber auch Unterschiede in Bezug auf Herkunft, Natur und einige andere Aspekte des Gesetzes. Alle Versuche in der Geschichte, die „menschliche Natur des Gesetzes“ zu verstehen, sind für uns sehr wertvolle Inspirationen. Wir sollten sie tiefgehend untersuchen und kritisch erben, damit die Studie über dieses Thema stets fortfahren kann.

Tabelle 1-4 Westliche Gedanken zur Menschlichkeitsbasis des Gesetzes

Schule	Repräsent. Person	Grundidee
Naturrechtswissenschaft	Aristoteles Cicero Hugo Gro Aquinas J. Rawls Th. Hobbes	Der Mensch ist die Kombination von Rationalität und Sensibilität. Die Erstere lässt Menschen virtuell agieren, und der letztere bringt Menschen dazu, böse zu handeln; Rationalität und Geselligkeit sind das, was den Menschen von anderen Tieren unterscheidet und sie sind auch das Wesen der menschlichen Natur; das Gesetz ist eben das soziale System, das diese Natur reflektiert und verwirklicht; das Naturgesetz ist das Gesetz der Moral und das Gesetz muss moralisch sein.

(Fortsetzung)

Tabelle I-4 Fortsetzung

Schule	Repräsent. Person	Grundidee
Philosophische Rechtskunde	I. Kant W. F. Hegel G. Radbruch	Die frühe philosophische Rechtskunde erbt die grundlegende Tradition der natürlichen Rechtskunde, suchte ebenso die Grundlage des Gesetzes aus der Moral des Menschen und nahm den Begriff des Naturrechts an. Stattdessen wurde das Naturrecht nicht als etwas in der wirklichen Existenz betrachtet, hat es dieses Gesetz jedoch als idealistisches oder philosophisches Gesetz ausgelegt, d.h. als Rechtsgrundsätze; die spätere philosophische Rechtskunde hat das Recht auch mit der menschlichen Natur in Verbindung gebracht, hat jedoch Unterschiede gemacht, indem sie die Auffassung der Entwicklung im Bereich der dynamischen Analyse der menschlichen Natur übernommen hat. Sie vertrat die Auffassung, dass die menschliche Natur sich entwickelt und verändert. In verschiedenen Zeiten variiert die menschliche Natur oder der menschliche Artentypus. Das Gesetz basiert auf der menschlichen Natur und unterscheidet sich also auch mit der Zeit.
--	Adam Smith David Hume	Der Mensch ist in der Natur egoistisch. Da die Menschen jedoch in der Gesellschaft leben müssen und ihr Erfolg von Interaktion und Zusammenarbeit mit anderen abhängt, ermöglicht dieser Prozess ihnen, Freundschaft mit anderen aufzubauen und dadurch Mitgefühl und Sympathie gegenüber anderen zu entwickeln und dann verschiedene Tugenden zu pflegen. Diese Tugenden sind einander nicht gleich. Und der Vorgesetzte würde sich weiter zu vollkommener menschlicher Natur entwickeln, während die minderwertigen die Gerechtigkeit sind, die die Grundlage ist, auf der die soziale Ordnung beruht und deren Aufrechterhaltung somit unvermeidlich ist.

Tabelle 1-4 Fortsetzung

Schule	Repräsent. Person	Grundidee
		Die Art und Weise, dies beizubehalten, ist es, falsche Täter zu bestrafen. Und das Gesetz übernimmt gerade diese Aufgabe. Was der Mensch weiß, ist alles, was der Mensch hat. Der Mensch hat zwei Arten von Bewusstsein, Freude und Schmerz. Dementsprechend, was der Mensch tut, ist „Schmerz zu vermeiden und Lust zu suchen“. Die Aufrechterhaltung der sozialen Stabilität und des Wohlstands erfordert die Einhaltung einiger Regeln und so entstehen die politische Macht und das Gesetz.
Utilitarische Rechtskunde und analytische Rechtskunde	Jeremy Bentham John Austin	Auf der Grundlage der Wahrnehmung der menschlichen Natur und der Nutzung der Natur, dass der Mensch „Schmerz vermeidet und Lust sucht“, verabschiedet das Gesetz die beiden Methoden der Belohnung und Bestrafung, um die Menschen dazu zu bringen, die Dinge im Einklang mit der moralischen Anforderung zu tun, nämlich die Dinge, die dem „maximalen Wohlbefinden der größten Mehrheit der Menschen“ förderlich sind. Das Gesetz ist in der utilitaristischen Natur des Menschen verwurzelt.
Soziale Rechtskunde	Roscoe Pound	Obwohl das Gesetz auf Basis des Strebens nach Utilität entstand und auch dazu dient, konzentriert es sich aber nicht auf den vorübergehenden Nutzen von Einzelpersonen, sondern auf das, was in der Tat verschiedene sozialen Interessen einschließen kann. Das Gesetz soll solche Vorteile als Kriterien für Messung und Regelung anderer Interessen nutzen.

(Fortsetzung)

Tabelle 1-4 Fortsetzung

Schule	Repräsent. Person	Grundidee
Rechtskunde der wirtschaftlichen Analyse	--	Der Mensch ist in der Natur das „rationale Subjekt, das seine Selbstzufriedenheit maximiert“. Der Mensch verfolgt das als sein Ziel, was auf Utilität abzielt. Basierend auf dieser Theorie und mit Nutzeffekt als Wertorientierung reguliert das Gesetz die Handlungen der Menschen und veranlasst sie dazu, Verhaltensweise zu wählen, die der Gesellschaft nützlich ist, indem es die Transaktionskosten erhöht oder verringert.
Politische Liberalisten	Friedrich August von Hayek	Dem Wesen nach ist das Gesetz eine Art von sozialen Regeln, die zu sozialer Ordnung führen. Die soziale Ordnung ist spontan und infolgedessen entsteht das Gesetz als soziale Regel auch spontan durch Interaktionen zwischen den Individuen und aber nicht dadurch, dass es von den Menschen bewusst formuliert wurde.
	Karl Marx Friedrich Engels	Der Mensch ist eine Art von Tier mit sozialer Praxis, das gewisse Freiheit genießt. Das Gesetz ist die Handlungsregel der Menschen, die diesem Wesen entsprechen. Das Gesetz ist der Verhaltenskodex für Menschen, der von Managern in der Gesellschaft auf der Grundlage der solchen Kenntnisse eingeführt worden ist. Das Gesetz widerspiegelt den kollektiven Willen der überwiegenden Mehrheit der Gesellschaft.

Quelle: Yan Chunsheng: „Rechtsgrundlage aus Sicht der menschlichen Natur“, Verlag des chinesischen Rechtssystems, 2016

Es soll darauf hingewiesen werden, dass ein Einblick in das Wesen der Rechtssysteme nur erzielt werden kann, wenn wir das Bild des Menschen, das hinter dem Gesetz steht, deutlich sehen. Ebenso können wir nur dann verstehen, warum der Mensch in verschiedenen Gerichtsbarkeiten unterschiedliche Bilder hat, wenn wir das Bild des Menschen hinter

dem Gesetz auf der Grundlage logischer Anordnung sortiert haben. In der juristischen Forschung legen wir Wert auf die objektive Bewertung rechtlicher Phänomene, aber nicht auf die Analyse und Untersuchung des Menschenbildes hinter dem Gesetz. Wir betonen die technische Analyse von Rechtsregeln und ignorieren aber die Rechtmäßigkeit und Vernunft, die zu Passung von Regeln und Menschlichkeit führen. Wir schenken großen Slogan der Rechtssysteme Aufmerksamkeit, legen aber wenigen Wert auf die sorgfältige Analyse der Harmonie und Koordination zwischen der Entwicklung der Systeme und Entwicklung der menschlichen Natur. Als solche ist die analytische Rechtskunde höchstens ein Wissen der Regel oder Technik. Sie kann niemals die Höhe der Rechtsphilosophie erreichen und die grundlegenden Rechtsgrundsätze festlegen, die dauerhaft und allumfassend sind. Wenn wir uns allmählich in die theoretische Untersuchung der Datenrechte vertiefen, müssen wir auf jeden Fall in die Tiefe der menschlichen Natur gehen, eine Frage von höchster Bedeutung. Als eine Reihe von Regeln, die das Datenverhalten regulieren, muss das System der Datenrechte die Voraussetzung und Grundlage seiner Autorität, Effektivität und Rationalität aus der menschlichen Natur schaffen. Die juristische Forschung und die Gesetzgebung müssen unbedingt auch auf Annahmen über Objekte beruhen, die sie regeln will und dann wird eine Art von System, Regel und Gesetz auf der Basis dieser Vorhypothese des Menschen erstellt. Die Gesetzgebung zu Datenrechten soll auch Hypothese des Menschen vorlegen, die sie regeln will. Ohne Vorhypothese des Menschen könnte das „Datenrechtsgesetz“ zu einem „unbrauchbaren Gesetz“ und sogar zu einem „ungerechten Gesetz“ werden.

Abschnitt II Datenperson-Hypothese und Altruismus

Daten digitalisieren, neu definieren, verbinden und verändern alles in unserer Welt. Bald genug werden alle Menschen und Dinge in Form der Daten existieren. Daten werden die physische Welt ersetzen und dies wird zu Merkzeichen und Etikett der Persönlichkeit werden.

Die gesamten Produktionsverhältnisse der Gesellschaft werden durch Datenkraft und Datenverhältnisse geprägt sein. „Die Datenisierung ist nicht nur ein technologisches System und mehr als alles in Bit und Byte zu nennen, sie bedeutet auch eine Reorganisation der Produktions- und Lebensweise der Menschheit. Sie stellt ein soziales System dar, das sich gerade erneuert wird, und was noch wichtiger ist, erneuert oder rekonstruiert sie das gesellschaftliche Leben der Menschheit“ (Qiu Zeqi 2016, S. 184). Im gewissen Sinne existiert der Mensch in zwei Formen, nämlich die des natürlichen Menschen und die der Datenpersonen. Es gibt zwei Arten von Technologien für das Leben, die Biotechnik und die Datentechnologie. Die Existenz des natürlichen Menschen wird durch genetische Technologie transformiert. Das ist die Technologie für das Leben. Die Existenz der Datenpersonen als Existenz des soziologischen Wesens nimmt bestimmte Technologien und ihre Beziehungen als Vorbedingung. Die soziale Interaktion beruht auf der Technologie und die grundlegende Kommunikationstechnik ist die Datentechnologie. Wir verlassen uns jetzt untrennbar auf Daten und eine Paradigma-Revolution in der Datensoziologie mit dem Menschen als Zentrum ist still im Gange. Diese Revolution wird die menschliche Gesellschaft in ein Zeitalter bringen, in dem Macht und Rechte umstrukturiert werden und die Privatsphäre mit Teilhabe von Daten synergetisch und miteinander konkurrieren. Dies wird sowohl das Bild als auch die Konnotation und Epitaxie des „Menschen“ grundlegend verändern. In Zukunft ist es ganz wahrscheinlich, dass die menschliche Gesellschaft aus „natürlichen Menschen“, „Robotern“ und „Gen-editierten Menschen“ bestehen wird. Hier bezeichnen wir alle datensierten natürlichen Menschen, Roboter und „Gen-editierten Menschen“ etc. allesamt als „Datenperson“.

(I) Aufstellung der Hypothese der Datenperson

Der „Mensch“ im juristischen Sinne, nämlich das vom Gesetz vorgestellte oder dargestellte imaginäre oder realistische Bild des Menschen, war sowohl in der chinesischen als auch ausländischen Wissenschaftswelt stets

der Hotspot der verbreiteten Aufmerksamkeit.¹ In den letzten Jahren, als sich die gesetzliche Realität änderte, haben chinesische Gelehrte über den „Menschen“ in juristischer Hinsicht immer tief gehender studiert. Der Rechtsbegriff des Menschen wandelt sich immer: verfassungsmäßig vom „Mensch des Status“ zum „Mensch der Gleichheit und Freiheit“ (Yu Zhong 2009) und zivilrechtlich vom „abstrakten Mensch“ zum „konkreten Mensch“ (Xie Hongfei 2002); im Umweltgesetz vom „Wirtschaftsmensch“ zum „Öko-Mensch“ (He Xiaorong & Chen Quansheng 2009), im Sinne des Sozialrechts vom „atomisierten Mensch“ zum „sozialisierten Mensch“ (Zhu Xiaozhe 2002) und aus Sicht der Rechtskunde vom „Mensch der Ethik“ zur „Mensch der Wissenschaft“ (Shen Zhai 2011). Diese Studien haben sich mit den Veränderungen des Menschenbildes in Zweigesetzen befasst, aber nicht den gesamten Prozess der Entwicklung des „Menschen“ in allgemeiner rechtlicher Hinsicht aufgezeigt und können daher einige schwierige Probleme im Aufbau der Rechtsstaatlichkeit nicht lösen. Wir sind der Meinung, dass sich der Mensch rechtlich von „Wirtschaftsmenschen“ zu „Datenpersonen“ wandelt. Gleichzeitig wird die Form der Menschenrechte durch Digitalisierung umgestaltet. Dementsprechend sollte sich unser Ansatz für Menschenrechte dahin gehend ändern, dass er auf „Datenperson“ basiert. Dies macht es erforderlich, einen völlig neuen Begriff der digitalen Menschenrechte zu etablieren, entsprechende Menschenrechtsschutzmechanismen einzurichten und die notwendige rechtliche Gewährleistung für „digitale Menschenrechte“ bereitzustellen (Ma Changshan 2019).

Die Hypothesen des Wirtschaftsmenschen, politischen Menschen, Moralmenschen, Sozialmenschen und Kulturmenschen usw. sind zweifellos tief Sinnig. Aber sie greifen nicht tiefer in die menschliche Natur ein. Der Mensch ist eine Kombination aus mehreren Facetten. Unser Verständnis dafür muss auch umfassend und ganzheitlich sein. Was wir verfolgen, ist nicht partiell scharfe Einblicke in alle Aspekte des Themas. Wir müssen

1 Zum Beispiel haben die „juristische Person“ von Gustav Radbruch (Deutschland), „Person im Privatrecht“ von Hoshino Echi (Japan) und „Disziplin und Bestrafung“ von Michel Foucault (Frankreich) usw. detaillierte Analyse und Untersuchung der Veränderungen des Bildes der juristischen Person geliefert und Merkmale in der Entwicklung der juristischen „Person“ dargestellt.

„allseitig scharfe Einblicke darin haben“. Wir sollten weder die genannten Hypothesen der menschlichen Natur leugnen noch sie als eine ewige Wahrheit behandeln. Stattdessen sollten wir die Hypothesen der menschlichen Natur als ein offenes System, das sich ständig weiterentwickelt, betrachten und die Rationalität und Notwendigkeit menschlicher Verhaltensweisen aus einer breiteren Perspektive interpretieren. Dies liegt daran, dass im „Zeitalter der Big Data alle sozialen Beziehungen mit Daten in einer Welt, die aus Daten besteht, dargestellt werden können und der Mensch die Summe der verwandten Daten ist“ (Li Guojie 2014). Alle sozialen Beziehungen sind im Wesentlichen Datenbeziehungen, die mit dem Schutz der Privatsphäre und altruistischen Datenteilhabe eng verbunden sind. Die persönlichen Abhängigkeiten werden durch materielle Abhängigkeiten ersetzt.² Und die Entwicklung der Menschheit, Technologie und Daten bietet eine neue realistische Möglichkeit, „Menschen“ von der persönlichen Abhängigkeit von „Ding“ in der modernen Gesellschaft zu liberalisieren. Wie Karl Marx vorausgesagt hat, wird die menschliche Gesellschaft drei Hauptformen nacheinander erleben: Sie wird von einer Gesellschaft mit persönlicher Abhängigkeit zu einer Gesellschaft mit persönlicher Abhängigkeit von Ding übergehen und dann zu einer Gesellschaftsform fortschreiten, in der Menschen frei sind und sich allseitig entwickeln. Die moderne

- 2 Die Frage der menschlichen Entwicklung ist ein wichtiger Teil der marxistischen Philosophie über den Menschen. Karl Marx teilte in seiner Wirtschaftswissenschaft Manuskript in 1857 den Prozess der menschlichen Entwicklung in die Stufe der menschlichen Abhängigkeit, den Zustand der materiellen Abhängigkeit und die Stufe der umfassenden Entwicklung der menschlichen Freiheit. Die Beziehungen der persönlichen Abhängigkeit (die zunächst recht spontan waren) sind die ersten Gesellschaftsformen, in denen sich die menschliche Produktivität nur in geringem Maße und an isolierten Stellen entwickelte. Die persönliche Unabhängigkeit, die auf der materiellen Abhängigkeit beruht, ist die zweite große Form: Dort entwickelte sich zum ersten Mal ein System des allgemeinen sozialen Warenaustauschs, was zu universellen Beziehungen, vielfältigen Anforderungen und universellen Kapazitäten führte. Die freie Individualität, die auf der universellen Entwicklung der Individuen und der Dominanz ihrer kommunalen und sozialen Produktivität beruht, die zu ihrem sozialen Reichtum geworden ist, ist die dritte Stufe. Die zweite Stufe schafft Voraussetzungen für die dritte Stufe.

Technologie, die durch die Datentechnologie repräsentiert wird, verändert jedoch die Spur der Entwicklung der menschlichen Gesellschaft und bringt eine Abhängigkeit von „Daten“ vor, bevor Menschen völlig frei von ihrer Abhängigkeit von Personen und Materialien sind. Die Daten haben in jeden Winkel des gesellschaftlichen Lebens Einzug gehalten, indem sie das soziale Muster und die organisatorische Umgestaltung des Lebensverhältnisses, auf die sich die menschliche Existenz stützt, still geformt, gestaltet und verändert haben und die Menschheit in die Ära der digitalen Zivilisation führen, indem das kognitive Muster, die Verhaltensweise, die soziale Struktur und die Ressourcenkonfiguration der Menschheit umgeschrieben werden.

Die gegenwärtige Gesellschaft befindet sich in der rapiden Veränderung der „Länder auf Autorädern“ zu „Ländern im Cyberspace“. Und diese Änderung erfordert Änderungen der „Spielregeln“ im Sozialleben der Menschen, d.h. eine „Staatsreform“ (Laura E. Quarantiello 1999) ist erforderlich. In dieser Zeit drängen Gesetz und Algorithmus, Ethik und Technologie sowie Regel und Moral gemeinsam auf eine neue Ordnung, während die Gesetzeszenarien tief greifende Veränderungen erfahren. Bei der Auseinandersetzung mit der Natur der „Datenpersonen“ fehlt es eindeutig an vorhandenen Kenntnissen und theoretischem Modell sowie an Auslegungskraft und Vitalität von ethischen und rechtlichen Rahmenbedingungen. In diesem Zusammenhang ist es zwingend erforderlich, eine neue Dimension des „guten“ Gesetzes zu schaffen, um die Notlage zu überwinden, mit der sich das Prinzip „Rechte haben Vorrang“ konfrontiert sieht und zu dem „verpflichtungsbasierten“ Ansatz des Rechts zurückzukehren, der das Problem der durch den „rechtsbasierten Ansatz“ verursachten „Funktionsstörung der Rechte“ lösen wird. Die Datenperson-Hypothese stellt eine theoretische Voraussetzung für Schaffung der Dimension des „guten“ Gesetzes dar und fügt der Menschlichkeitshypothese des Gesetzes in der Big-Data-Ära einen rationalen Faktor hinzu.

Datenperson ist die brandneue Darstellung der menschlichen Natur in der Big Data Ära. Die Geschichte hat bewiesen, dass jeder Fortschritt der Menschlichkeit eine beispiellose Auswirkung auf die Gesetzgebungsansicht und deren Wertverfolgung hatte. Im Zeitalter des Privatrechts ist der Mensch im Rechtssinne der „Wirtschaftsmensch“. Dann entstand das

Sozialrecht auf der Grundlage von Reflexionen über den Egoismus des „Wirtschaftsmenschen“³ und der Entdeckung von Sozialität und Altruismus in der menschlichen Natur. Es ist zweifellos eine bedeutende Wende in der Geschichte der Rechtskunde. Aber das bedeutet keineswegs die letzte Wende, weil sich die menschliche Natur mit der Zeit weiter verändern, entwickeln und verbessern wird. Gegenwärtig treten globale Datensicherheitskrisen immer wieder auf, da die Spannung zwischen Menschen und Technologie, Menschen und Wirtschaft sowie Menschen und Gesellschaft zunimmt und sich vertieft. In diesem Zusammenhang stellt die Menschheit erneut fest, dass die Hypothese des „Sozialmenschen“ usw. unter anderem nicht mehr ausreicht, um die Konflikte zwischen Menschen und Daten zu lösen. Und es ist notwendig, bestehende Barrieren und Grenzen durch tiefere Reflexionen herauszufordern und zu überwinden. Der „Datenmensch“ ist das, was wir nach solchen Reflexionen entwickelt haben. Das ist eine völlig neue Darstellung der menschlichen Natur in der Big Data Ära.

- 3 Wirtschaftswissenschaftler haben nach und nach erkannt, dass die Hypothese des Wirtschaftsmenschen, die ein Modell des definitorischen Denkens darstellt, in unserer Zeit der intelligenten Entwicklung und Informatisierung vor großen Herausforderungen steht und die in der Realität vorhandenen altruistischen Verhaltensweisen nicht erklären kann, was den Gegenbeweis der Unzulänglichkeit der Hypothese des Egoismus direkt antreten kann. Wir sollen offen die Grenzen und die Unfähigkeit der Hypothese des Wirtschaftsmenschen zugeben. Wir sollen den Wirtschaftsmenschen nicht leugnen, sondern nur über ihn hinausgehen (Siehe Yang Chunxue: „Wiedergeburt‘ des Wirtschaftsmenschen: Untersuchung und Verteidigung für eine neue Zusammenfassung“, in „Wirtschaftsforschung“, 11. Ausgabe, 2005). Aus Sicht der Wirtschaftsphilosophie befindet sich die Doktrin des rationalen Egoismus in einem nicht lösbaren Dilemma, wenn man versucht, Probleme im Zusammenhang mit dem gegenwärtigen wirtschaftlichen Verhalten zu erklären, und stößt auf Herausforderungen aufgrund von Ungleichgewicht, Informationsasymmetrie und häufigem Auftreten von Unsicherheiten der Marktwirtschaft im 20. Jahrhundert. Darüber hinaus hat die Menschheit deshalb überlebt, gedeiht und glorreiche Zivilisationen geschaffen, liegt nur daran, dass der Mensch nicht vollständig egoistisch ist und voller altruistischer Gefühle für Verwandte, Freunde und sogar Fremde ist. Man kann sagen, ohne das altruistische Verhalten der Menschen hätte die menschliche Entwicklung nicht das erreicht, was sie heute erreicht hat.

Mit der Aufstellung der Datenperson-Hypothese⁴ gehen wir über die traditionelle Grenze zwischen Gut und Böse hinaus, brechen von den traditionellen Fesseln ab, die die gemeinsame Nutzung von Daten einschränken und betonen den Altruismus in Beziehungen der menschlichen Verhaltensweisen und in der Form der Existenz. Die „Datenperson“, die auf Altruismus und Gemeinnutzung basiert, verfolgt, erschafft und realisiert den Datenwert, wobei er dem Grundprinzip der Datenwertmaximierung folgt. Seine grundlegende Konnotation ist das Gleichgewicht zwischen rechtmäßigem Schutz und angemessener Nutzung von Daten. Anders als die egoistische Natur des Wirtschaftsmenschen vertritt die Datenperson als Altruist all den Geist der Gemeinnutzung. Die Datenperson-Hypothese bestätigt sowohl die Rationalität bei der Verfolgung von Gewinn durch verschiedene Interessenträger, betont als auch die Notwendigkeit der Zusammenarbeit und Gemeinnutzung, die dem Erfordernis der Entwicklung der Datenkraft und der Reform der Datenverhältnisse entspricht. Daher sind wir der Ansicht, die menschliche Natur der Datenphilosophie als „Datenperson“, die die Vereinheitlichung des Datenschutzes und der Datenverwendung verkörpert, voranzunehmen. Wir nehmen diese Hypothese als den Ausgangspunkt der Analyse und Prämisse für die logische Schlussfolgerung in der Theorie der Datenrechte.

Die Basis des Gesetzes ist Person, deren Anforderungen und Erwartungen an das Gesetz sich ständig ändern und entwickeln. „Jede soziale

- 4 Die Entstehung der Datenperson-Hypothese ist notwendig und unvermeidlich. Erstens kann sie die bestehende Struktur der menschlichen Natur ändern, d.h. von einer Struktur, die sich auf den Wirtschaftsmenschen oder den Sozialmenschen konzentriert, zu einer Struktur ändern, die sich auf den Datenpersonen konzentriert und ein dynamisches Gleichgewicht anstrebt. Zweitens ermöglicht es, das bestehende Rechtssystem zu überprüfen, ein institutionelles System zu schaffen, das für die Entwicklung der digitalen Gesellschaft geeignet ist, das Datenrechtssystem auf der Grundlage eines pluralistischen Menschlichkeitssystems aufzubauen und die Basis für Regulierung des Datenverhaltens der Menschen und für ein besseres Leben für die Menschheit stärken. Drittens können wir keine Datenrechtstheorie aufbauen, die mit dem System der Wirtschaftstheorien vergleichbar ist, wenn wir keinen Durchbruch in der Theorie und Philosophie der Datenpersonen erzielen können.

Umwälzung führt zu veränderten Anforderungen des Menschen und jede Änderung der Zeit führt auch dazu, dass die Menschen unterschiedliche Erwartungen an das Gesetz haben. Deshalb ist die Geschichte der Entwicklung und Evolution des Gesetzes in großem Maße die Geschichte der ständigen Entwicklung und Veränderung des Bildes der gesetzlichen Person“ (Hu Yuhong 2008, S. 16). Das Modell der Rechtsperson liefert eine „Skizze“ der gesetzlichen Person, bei der es sich um das Bild der Rechtsperson handelt, das aus der Verallgemeinerung und Kategorisierung der gesetzlichen Person hervorgeht (Wu Xianjing 2010). Gegenwärtig werden Datensicherheitsrisiken immer markanter, Fälle von Datenrechtsstreitigkeiten treten immer häufiger auf und die digitale Zivilisation ist im Entstehen begriffen. Vor diesem Hintergrund ist es notwendig und unvermeidlich, dass sich das Modell der Datenperson zum Modell der Rechtsperson entwickelt. Die Datenperson befindet sich in dem Rechtsszenario, das durch den Aufstieg des Datenrechtsgesetzes dargestellt wird. Das Datenrechtsgesetz stellt das Gesetz dar, das sich auf Dateneigentumsrecht, Datenrecht, Datennutzung und Datenschutz bezieht. Die größte Bedeutung dieses Gesetzes besteht darin, „Daten bestmöglich zu nutzen, ihre Aufteilung festzusetzen und Konflikte und Streitigkeiten zu verhindern“. Das Auftauchen von Problemen im Zusammenhang mit Datensicherheit und Dateneigentumsrecht etc. ist für das Datenrechtsgesetz insofern von größter Bedeutung, als sie neue rechtliche Fakten liefern, die mit dem Datenrechtsgesetz angepasst werden müssen. Im Rahmen des Gesetzes geht es bei Datenrechten nicht nur um das Verteilungsverhältnis von Datenrechten und -interessen, sondern auch um das Verhältnis, wie man Daten verwendet und schützt etc. Diese beiden Arten von Verhältnissen können nicht vom traditionellen Modell der Rechtsperson abgedeckt werden. In einer Zeit, in der sich Datensicherheitskrisen auf der ganzen Welt ausbreiten und das Datenrechtsgesetz so entsteht, wie es sollte, müssen wir unser traditionelles Verständnis des Menschen in juristischer Hinsicht überdenken. Wie das Bild der gesetzlichen Person aufgebaut werden soll und wie sich das Modell der Rechtsperson entwickeln soll, sind theoretische Aufgaben, die unsere Forschung zum Datenrechtsgesetz erfüllen muss. Die menschliche Natur legt die philosophische Grundlage für das Datenrechtsgesetz und aus ihr ergibt sich auch die Ausdrucksweise des Systems. Unsere ursprüngliche

Absicht ist es, das Datenrechtsgesetz – ein völlig neues historisches Phänomen in der Rechtswelt auf dem grundlegenden Forschungsparadigma von der gesetzlichen Person und dem Modell der Rechtsperson, zu erläutern. Außerdem werden wir den Grundgeist, das Grundprinzip und das Grundsystem des Datenrechtsgesetzes durch einen Vergleich der Gleichheit und Verschiedenheit zwischen der Person im Datenrechtsgesetz und der anderen Rechtsperson darlegen.

Natürlich kann jedes Modell das Problem der übermäßigen Vereinfachung des vorliegenden Problems mit sich bringen. Und die Beschreibung der gesetzlichen „Person“ mit dem „Wirtschaftsmenschen“ oder der „Datenperson“ können natürlich nicht alle Aspekte des Gesetzes abdecken. Tatsächlich hat die gesetzliche „Person“ im modernen Gesetz mehrere Bilder dargestellt. In Zukunft könnte die gesetzliche „Person“ wahrscheinlich vor allem zum Bild der „Datenperson“ werden, während andere Facetten lediglich Modifikationen oder Ergänzungen dazu sein werden. Die Verlagerung der rechtlichen Annahme des „Menschen“ vom „Wirtschaftsmenschen“ zur „Datenperson“ bedeutet, dass das Gesetz von den Menschen verlangt, eine brandneue Denkweise im Leben anzuwenden. Da der Übergang vom „Wirtschaftsmensch“ nun zur „Datenperson“ eine Entscheidung ist, die wir aus eigener Initiative treffen, müssen wir als Nächstes die „Datenperson“ von der Theorie in die Praxis bringen.

(II) Datenperson und Altruismus

Das Wort „Altruismus“ wurde zuerst von Auguste Comte, einem französischen Philosophen und Ethiker des 19. Jahrhunderts, vorgeschlagen. Ausgehend vom Instinkt und der Natur der Menschheit illustrierte er die Rationalität des Altruismus. „So wie es rationale Anforderungen an das Denken gibt, gibt es rationale Anforderungen an das Verhalten. Und der Altruismus ist eine der rationalen Anforderungen daran“ (Thomas Nagel 1978, S. 3). Der Altruismus wurde in Bereichen wie Biologie, Soziologie, Psychologie und Ökonomie etc. untersucht und aus verschiedenen Perspektiven von diesen Disziplinen definiert. Als ein soziales Tier kann der Mensch nicht völlig egoistisch handeln, um die Zusammenarbeit

aufrechtzuerhalten und zu verbessern. In jedem Zeitalter ist daher der altruistische Geist notwendig und wird in der sozialen, kulturellen und institutionellen Entwicklung befürwortet und das altruistische Verhalten soll als guter und wichtiger Wert angesehen werden. Wir nennen diesen Wert Altruismus. Der in der Antike gereifte Altruismus war im Mittelalter vorherrschend und bleibt in der Neuzeit und Gegenwart immer noch relativ einflussreich. Zu den repräsentativen Persönlichkeiten zählen unter anderem Konfuzius, Mozi, Jesus und Immanuel Kant usw. In Bezug auf die menschliche Natur glaubten sie, dass der Zweck des Verhaltens jedes Einzelnen selbstlos und altruistisch sein kann. Von Platons Utopie, Jean-Jacques Rousseaus Gesellschaftsvertrag bis zu Peter Kropotkins Theorie der gegenseitigen Hilfe betonten sie alle, dass der Mensch von Natur aus gut sei, wenn er nicht korrumpiert wäre.⁵ Das Gebot, „wir sollen bessere Menschen werden“, klingt unvermindert in unserer Seele (Immanuel Kant 2003, S. 33). Die traditionelle chinesische Kultur mit dem Konfuzianismus als Vertreter, betonte den Gesamteffekt und Altruismus. Laut Mencius zum Beispiel ist jeder von Natur aus mit Altruismus ausgestattet und jeder hat die Fähigkeit, altruistisch zu handeln.

Die altruistischen Verhaltensweisen der Menschheit sind das universelle Ergebnis der biologischen Evolution und der gesellschaftlichen Entwicklung zusammen. Die Zusammenarbeit ist für die Menschheit so wichtig, dass „ein Mensch sehr schwer Sympathie von einigen wenigen Personen gewinnen kann, obwohl er sich für das ganze Leben darum bemüht, während es für ihn in der zivilisierten Gesellschaft notwendig ist, jederzeit die Mitwirkung und Unterstützung großer Menschenmassen zu bekommen“ (Adam Smith 1997, S. 13). Die Zusammenarbeit durchdringt alle Dimensionen, alle Bereiche und alle Regionen unseres sozialen und wirtschaftlichen Lebens und verläuft durch die Entwicklung der ganzen menschlichen Gesellschaft (Huang Tao 2009). In „The

5 Karl Marx und Friedrich Engels wiesen wiederholt darauf hin, dass der Kapitalismus und alle früheren sozialen Formen gegen die menschliche Natur verstießen. Dies zeigt, dass die menschliche Natur in ihren Köpfen ursprünglich das feine und freundliche Attribut des Menschen war und nur durch Privateigentum und Klassenunterdrückung entfremdet wurde. Die menschliche Natur als gut zu interpretieren, entspricht ihrer ursprünglichen Absicht.

Wealth of Nations“ benutzte Adam Smith nicht nur das Beispiel für Herstellung von Anstecknadel, um die Bedeutung der Arbeitsteilung zu veranschaulichen, sondern auch einige andere Beispiele, um die Bedeutung der Zusammenarbeit darzulegen: Zum Beispiel „Die stümperhafte Wolljacke, die den Tagelöhner bedeckt, ist das Produkt der gemeinsamen Arbeit einer großen Menge Arbeiter. Der Schäfer, der Wollpflücker, der Wollkämmer oder der Färber, der Schreiber, der Spinner, der Weber, der Bleicher, der Schneider mit vielen anderen, müssen alle ihre verschiedenen Künste verbinden, um auch dieses heimliche Produkt zu vollenden“ (Adam Smith 1997, S. 11). Herbert Simon definierte den Kooperationsgeist als gute Tugend wie die soziale Toleranz, Sympathie, Hilfsbereitschaft, Leidenschaft, Moral etc. Durch diese Eigenschaften opfert ein Individuum zuerst seine Lebensbehaglichkeit. Aber weil dieser Altruismus die durchschnittliche Lebensbehaglichkeit der ganzen Gesellschaft erhöht, fördert die Gesellschaft wiederum solche altruistische Verhaltensweise (Wang Dingding 2005, S. 199). Auf der Grundlage der Einführung in die neuesten Forschungsergebnisse von Herbert Gintis, einem amerikanischen Ökonomen und anderen, wies der Gelehrte Wang Dingding und andere darauf hin, dass die Kooperationsordnung der Menschheit immer existiert und weit verbreitet ist. So ist es für jeden Einzelnen die Zusammenarbeit besser als die Nichtkooperation. Deshalb ist die Zusammenarbeit nicht gegen die Grundprinzipien der Biologie und Ökonomie. Alle selbstsüchtigen Individuen wollen lieber kooperieren als nicht. Kooperation bedeutet Koexistenz von Egoismus und Altruismus (Wang Dingding 2005, S. 204). Die Zusammenarbeit liegt auf der tiefgehendsten Grundlage der Zusammensetzung und Existenz der menschlichen Gesellschaft. Infolge der Arbeitsteilung und der Zusammenarbeit ist es für die Verhaltensweisen der Menschheit notwendig, mit anderen als Mittel die Zusammenarbeit durch andere Menschen zu erfüllen. So kann man sagen, der Altruismus ist ein effektiver Weg, um Ziel zu verwirklichen. Die Zusammenarbeit schafft Synergie. „Die Frage hier ist nicht nur, dass die individuelle Produktivkraft durch die Kooperation erhöht, sondern auch eine neue Produktivkraft geschaffen worden ist. Und diese Produktivkraft ist unausbleiblich die kollektive Kraft“ (Central Compilation and Translation Bureau 1972, S. 362).

Das Big-Data-Zeitalter erfordert die Etablierung des altruistischen Geistes. Die Struktur der Beziehungen in der digitalen Gesellschaft bestimmt, dass der inhärente Mechanismus einer solchen Gesellschaft die dezentralisiert, abgeflacht und grenzenlos ist und dass ihr Grundgeist die Offenheit, Teilhabe, Zusammenarbeit und gegenseitiger Nutzen ist. Das bedeutet, dass eine solche Gesellschaft zwangsläufig „menschenorientiert“ ist und dass der Kernwert des „Altruismus“ in dieser Ära auch dadurch bestimmt ist. Ein riesiger Kooperationsüberschuss bringt den altruistischen Geist hervor, während der Altruismus Menschen aus dem Dilemma für Gefangene herausführen kann. Der Egoismus und Altruismus bildet eine dialektische Einheit. Wollte jemand egoistisch sein, muss er zuerst altruistisch handeln. Nur durch Altruismus kann man besser egoistisch handeln.⁶ Jack Ma hat einmal in einer Rede gesagt, dass „die Menschheit vom IT-Zeitalter ins DT-Zeitalter übergeht“ und dass der Altruismus das Kernstück dieses Zeitalters darstellt. Ihm zufolge sollte man „glauben, dass andere wichtiger, klüger und fähiger sind als du; und dass du ohne den Erfolg der anderen nicht erfolgreich sein kannst.“ Altruismus und Gemeinnutzung sind besser als Egoismus und Exklusivität; und der Altruismus ist der Kern der Zukunft.

Die Evolution der menschlichen Natur wird unweigerlich Veränderungen des Wertes des Gesetzes herbeiführen. Die Datenperson stellt eine brandneue Version der menschlichen Natur in der Big Data Ära dar. Das bedeutet, dass sich unser „Selbst“ zu einem „Großselbst“, das eine Integration von Mensch und Daten ist, entwickelt und dass der altruistische Geist nicht nur im physischen Raum vorherrscht, sondern auch über die Kategorie der Menschheit hinausgeht und damit Ordnung in den virtuellen Raum bringt. Die traditionelle Ordnung ist zentralisiert, hierarchisch und exklusiv, während die neue Ordnung auf einer dezentralisierten, abgeflachten und offenen Grundlage beruhen wird. Dies bestimmt, dass das Wesen der Datenperson Altruismus und Gemeinnutzung ist. Die menschliche Natur

6 Amerikanischer Ökonom Milton Friedman, Nobelpreisträger in der Ökonomie, sagte einmal treffend, dass er vor dem Lesen des Reichtums der Nation keine Ahnung hatte, was „Egoismus“ sei, und dass er erst nach dem Lesen der Theorie der moralischen Gefühle verstanden habe, dass der „Altruismus“ mit einem klaren Gewissen „Egoismus“ bedeutete.

ist immer mit den Charakteristiken der Zeit geprägt und wird unweigerlich die Entwicklung und Evolution des Wertes des Gesetzes nach der Strömung des Zeitalters vorantreiben, da die Räder der Geschichte sich unaufhörlich vorwärts bewegen. Die Veränderung der menschlichen Natur im Zeitalter der Big Data, die durch Datenperson repräsentiert wird, wird sicherlich und letztendlich zur Veränderung der gesetzlichen Sicherheit, des Wertes der Gemeinnutzung und des Altruismus führen.

(III) Möglichkeit des Altruismus

In „The Theory of Moral Sentiments“ wies Adam Smith zu Beginn klar auf die altruistische Natur des Menschen hin, „Wie egoistisch einer nach der Meinung der anderen auch sein mag, so gibt es offenbar einige Prinzipien in seiner Natur, die ihn an das Glück der anderen interessieren und ihr Glück für ihn notwendig machen, obwohl er nichts davon ableitet, außer der Freude, das Glück der anderen gesehen zu haben“ (Adam Smith 2015, S. 5). „Obwohl ihr einziges Ziel darin liegt, ihre langweilige und unersättliche Wünsche zu befriedigen, indem sie tausende Menschen anstellen und für sie arbeiten lassen, verbrauchen sie aber gleich wie die Armen den Erfolg, den sie durch alle Reformen erzielt haben. Sie werden von einer unsichtbaren Hand geführt, um fast die gleiche Verteilung der Grundbedarfsgüter des Lebens zu machen, wie die Erde unter allen ihren Bewohnern in gleiche Teile geteilt werden konnte und sie haben damit ohne es zu wollen, ohne es zu wissen, die Interessen der Gesellschaft gefördert und auch Lebensmittel für immer vermehrende Menschen geliefert“ (Adam Smith 2015, S. 234). In der Natur des Menschen ist eine Tendenz und Trends zu geheimer Liebe zu anderen (Francis Bacon 1983, S. 36). Der Altruismus ist keine Illusion. Es ist nicht nur notwendig als auch möglich. In der modernen Gesellschaft gibt es offensichtlich Altruismus unter drei Umständen: die Bereitschaft, die eigene Zeit, Energie und Reichtum im Austausch gegen bestimmte unmittelbar sichtbare Interessen anderer, bestimmte zukünftige Interessen anderer und bestimmte eigentlich nichtige Interessen anderer zu verbrauchen und aufzuwenden (Cheng Enfu 1997, S. 151–161).

Altruismus ist gut für die ganzheitliche Entwicklung der Menschen. Nach Abraham Maslow's Hierarchie der Bedürfnisse neigen diejenigen, die sich in der Hierarchie der Bedürfnisse auf niedrigen Ebenen befinden, dazu, egoistische Verhaltensweisen zu zeigen, während die Bedürfnisse auf höheren Ebenen nur durch Zusammenarbeit und gemeinsame Nutzung befriedigt werden können. Ein gewisses Maß an Altruismus ist daher zur Befriedigung solcher Bedürfnisse notwendig. „Je höher er in der Hierarchie des Bedarfs liegt, je mehr er oder sie die natürliche Neigung zur Teilhabe aufdeckt“ (Wang Tianen 2018). Je höher das Niveau der Bedürfnisse, desto mehr muss man teilhaben und altruistisch sein, um sie zu erfüllen. Nachdem die Bedürfnisse auf den niedrigen Ebenen befriedigt sind, wird man allmählich die Leiter auf die Stufe der Selbstaktualisierung hinaufsteigen und bis dahin wird es Chancen und Möglichkeiten geben, den Konflikt und die Spannung zwischen Egoismus und Altruismus zu lösen. Wenn also nur die grundlegendsten materiellen Bedürfnisse verfolgt werden, ist es vernünftig, die Maximierung der persönlichen Interessen anzustreben. Sobald er jedoch die Hierarchie der Bedürfnisse erhöht, werden Egoismus und Altruismus nicht mehr miteinander konkurrieren. Stattdessen fühlt es sich an, als ob sich der Egoismus in den Altruismus eingeschmolzen worden wäre.

Die menschliche Gesellschaft braucht Altruismus. Seit der Antike sind die Menschen aufeinander angewiesen, um zu überleben, und kein Mensch ist eine Insel. So wie Karl Marx es ausdrückte, „kann der Einzelne nur im Kollektiv die Mittel erwerben, um seine Talente in einem Allround-Game zu entfalten“. In der Zusammenfassung seiner Leistungen sagte Isaac Newton einmal, dass „es ist, wenn ich etwas weiter als einige andere sehen kann, weil ich auf den Schultern von Riesen stehe.“ Dies impliziert, dass Altruismus unter Individuen (unter anderem Klassenkameraden, Freunde und Mitarbeiter usw.) absolut notwendig ist. Da die Arbeitsteilung verfeinert wird und die Ketten die Menschen enger als je zuvor verbinden, werden die Interessen des Einzelnen durch Befriedigung der Bedürfnisse anderer, also der Gemeinde und der Nation verwirklicht. Wenn jeder nur die Maximierung seiner persönlichen Interessen verfolgt und die Interessen anderer nicht im Auge behält, würden wir uns im „Hobbes Dschungel“ wiederfinden und nicht mehr herausgehen können. Gegenseitiger Schaden

in der Gesellschaft ist im Wesentlichen das Ergebnis der Kurzsichtigkeit des übermäßigen Egoismus und, wenn nicht reguliert, würde er sich entwickeln und zu einer gegenseitig schädigenden Gesellschaft führen. Im Gegensatz dazu, wenn jeder bereit ist, einen Teil seiner eigenen Interessen für die Interessen anderer abzutreten, wird eine Gesellschaft von "alle für einen und einer für alle" möglich werden. In einer digitalen Gesellschaft müssen wir mehr tun, um die Menschen zu altruistischen Verhaltensweisen zu führen, um die gesunde, geordnete, harmonische und nachhaltige Entwicklung der Gesellschaft zu gewährleisten.

Obwohl Probleme bei der globalen Datenregulierung der Menschheit beispiellose Krise und Einschränkung der Datensicherheit bringen, werden die Notwendigkeit und Möglichkeit dafür aber gleichzeitig auch sichtbar, dass die Menschheit Strategie von „Zusammenarbeit-Altruismus“ wählt, um solche Krise und Einschränkung loszuwerden. Laut Martin Nowak, Biologe an der Harvard University, „ist Kooperation der Architekt der Kreativität in der gesamten Evolution, also alles von Zellen über multizelluläre Kreaturen bis hin zu Ameisenhaufen und von Dörfern bis zu Städten ohne Ausnahme“. Wenn die Menschheit sich auf die neuen Herausforderungen der globalen Verwaltung vorbereitet, muss sie neues Kooperationsmodell finden und Altruismus sollte die Grundlage für Zusammenarbeit sein. Was die Länder betrifft, können sie nur dann ermöglichen, dass alle Interessenträger ihre Dateninteressen maximieren, wenn sie zusammenarbeiten, den Grundsatz der Dateninteressenübertragung befolgen, Anpassung oder Gleichgewicht zwischen den jeweiligen Dateninteressen der verschiedenen Länder und Nationen und den Interessen der Datengemeinschaft mit einer gemeinsamen Zukunft für die Menschheit suchen. Natürlich ähneln alle Interessenparteien als Handlungsträger in der internationalen Aktivität, was die Dateninteressen betrifft, dem „Wirtschaftsmenschen“, der eine gewisse Zeit lang die Maximierung der Dateninteressen anstrebt. Es kann aber nicht immer eine Gemeinsamkeit oder ein Gleichgewicht zwischen den Dateninteressen realisiert werden, und der Verrat an der Datenzusammenarbeit ist oft nichts Ungewöhnliches. Dazu ist es notwendig, eine Reihe wirksamer internationaler Regeln für die Verarbeitung von Daten zu erarbeiten, um solche Handlungen zu spezifizieren, damit die internationale Zusammenarbeit im Bereich der Daten langfristig erhalten werden kann.

Wenn die menschliche Natur nichts anderes als böse sein könnte, wären diejenigen, die das System entwerfen, sicherlich auch böse. Solche Böse könnten jedoch kein gutes System schaffen. Trotzdem ist es für uns absolut möglich und wir sind auch definitiv in der Lage, das Böse aufzugeben, die „Bestialität“ in der menschlichen Natur loszuwerden und das Gute zu verstärken. Zumindest können wir die Möglichkeit und Neigung vermeiden, böse Dinge zu tun. Die Sozialität des Menschen ist der Boden, auf dem der Altruismus wächst, und insbesondere die Notwendigkeit der Zusammenarbeit liefert eine direkte Motivation für den Altruismus. „Eine Person, die den Prozess der Sozialisierung erlebt hat, besitzt nicht nur die angeborenen egoistischen Motive, sondern auch die altruistischen Motive, die durch nachfolgende Werteinternalisierung gebildet werden, während die anschließend gebildeten altruistischen Motive die egoistischen Motive zurückhalten und umgestalten“ (Guo Jing 2005). Die Geschichte zeigt, dass die Menschheit seine Elemente wie Rohling, Gier und Selbstsucht usw. mit der Entwicklung der Gesellschaft und dem Fortschritt der Zivilisation allmählich reduziert und seine altruistische Mentalität, sein inneres Gesetz und die Idee der Gemeinnutzung etc. dadurch zunehmen und zum Hauptthema des Lebens werden und die Menschheit so einen vom Altruismus dominierten Entwicklungsweg betritt. In der menschlichen Gesellschaft ist es ein Ideal, dass jeder Altruismus als Verhaltenskodex betrachtet. Als Datenressourcen und -produkte am reichlichsten vorhanden sind und je nach Bedarf verteilt werden können, werden die Ideen von Gerechtigkeit und Gemeinnutzung an Popularität gewinnen, während die Datenbearbeitung zum Mittel für ein glückliches Leben, der Altruismus stark zunehmen wird und der Egoismus und Altruismus eine perfekte Einheit bilden. Mit dem Wandel der Zeit und der Entwicklung der Gesellschaft wird der Wert des Altruismus immer wichtiger und sichtbarer und der Altruismus als Blüte der Zivilisation wird sicherlich in voller Blüte stehen.

Laut Thomas von Aquin dient das Gesetz dem Gemeinwohl. Bei der Gestaltung des Datenrechtssystems muss man den Altruismus in der menschlichen Natur berücksichtigen, alles tun, um das Gute in der menschlichen Natur zu fördern und anzuspornen und gleichzeitig die Möglichkeit zu unterdrücken, dass der Mensch zum Bösen neigen könnte. Der Altruismus ist die menschliche Grundlage des Datenrechtsgesetzes und damit

der Ausgangspunkt und Endpunkt der Formulierung und Umsetzung des Datenrechtsgesetzes. Als Rechtssystem für Anpassung von dem Eigentum, Recht, der Nutzung und dem Schutz von Daten und die Grundnorm für das datenbezogene Verhalten und Aufrechterhaltung der Datenordnung soll das Datenrechtsgesetz wesentlich darauf abzielen, ein Gleichgewicht und eine Koordinierung zwischen wirksamem Schutz der Datenrechte und bestmöglicher Nutzung der Daten, Wahrung der öffentlichen Interessen und der öffentlichen Sicherheit bei gleichzeitiger Förderung der freien Teilhabe personenbezogener Daten zu realisieren. In diesem Zusammenhang ist die Übertragung von Datenrechten durch Bürger bis zu einem gewissen Grad von entscheidender Bedeutung für die Verwirklichung eines Gleichgewichts und einer Koordinierung zwischen gesetzlichem Schutz und angemessener Nutzung von Daten.

Das heißt, die Gesetzgebung zu Datenrechten soll den Datenfluss und die Nutzung von Daten fördern, anstatt den Daten durch die Verbreitung einer gesetzlichen Masche Beschränkungen aufzuerlegen. Wie Gustav Radbruch einmal sagte: „Es ging dem Rechtssystem nicht darum, die Menschen dazu zu bringen, ihre Augen jederzeit wie Wachposten zu fixieren, sondern ihnen zu ermöglichen, gelegentlich und sorglos zu den hellen Sternen, Blumen und Bäumen in voller Blüte aufzublicken sowie die Notwendigkeit der Unbeschränktheit und Tugenden auch zu gucken“ (Gustav Radbruch 2001, S. 9). Der Altruismus ist die menschliche Grundlage oder menschliche Dimension des Datenrechtsgesetzes, was bedeutet, dass das Datenrechtsgesetz mit dem Altruismus als sein Ausgangspunkt die altruistischen Anforderungen vermittelt, mit dem Altruismus als sein Hauptinhalt und das vom Altruismus anstrebende ultimative Ziel – Gemeinnutzung als sein höchstes Wertziel, das es verfolgt und in erster Linie darauf abzielt, den Altruismus der Menschen zu modellieren und zu fördern. Aber dies bedeutet natürlich nicht, dass das Datenrechtsgesetz keine anderen Wertziele wie Sicherheit, Effizienz, Nutzen und Ordnung etc. verfolgt. Der Schlüssel hier ist, dass diese Wertziele den Platz des Altruismus als Ziel nicht ersetzen sollen.

Im Gefolge davon, dass die Idee der Teilhabe die Popularität der Menschen immer gewinnt, wird der Altruismus, der in der menschlichen Natur verborgen ist, allmählich heraus angeregt. In gewissem Sinne spielt das

Datenrechtsgesetz die Rolle einer „Hebamme“ für Altruismus und trägt zur Förderung des altruistischen Geistes bei. „Die Menschheit kann echten Altruismus entwickeln“ (Holmes Rolston 2000, S. 465). Die Formulierung des Datenrechtsgesetzes zeigt, dass die Menschheit das Verhältnis zwischen Menschen und Daten besser verstanden hat. Die Menschen sind sich dessen bewusst, dass sie nach dem Prinzip des Datentransfers, das am besten zur Steigerung der Gesamtinteressen der Gesellschaft geeignet ist, dass sie ihr Bestes tun soll, um das Wohlergehen der Daten in der Gesellschaft zu steigern. Für die Gesellschaft ist es gerecht, ein System zu schaffen, um den Inhalt der altruistischen Menschlichkeit zu bereichern, den altruistischen Geist unter den Menschen zu inspirieren und dann die Beziehungen zwischen Menschen und Daten weiter zu harmonisieren. Es ist begründet und völlig vernünftig, das Datenrechtsgesetz auf die Datenperson als Menschlichkeitshypothese zu stützen, da diese Hypothese nicht nur den neuen Einblick in die menschliche Natur beschreibt, die relevante Subjekte auf natürliche Weise präsentieren sollen, wie dies durch die grundlegenden Eigenschaften wie die Sozialität, den Altruismus und die Teilhabe des Datenrechtsgesetzes bestimmt wird, sondern auch Leitlinien für die wissenschaftlich fundierte Erstellung und wirksame Umsetzung des Datenrechtsgesetzes bieten kann, indem die Notlage der Datensicherheit bei der Datenverwaltung gemildert oder überwunden wird. Dies ist sowohl das, was unvermeidlich ist, wenn sich die Gesellschaft entwickelt, als auch das, was vor der Tür steht, wenn die Menschheit weiterhin Fortschritte macht.

Abschnitt III Das Datenrechtssystem und die Legalisierung von Datenrechten

Die „Neuvermischung“⁷ ist eine Kraft, die auf Änderungen drängt, die natürlich und zwangsläufig eintreten werden. Es hat beispiellose

7 Die sogenannte Neuvermischung bedeutet die „Neuordnung und Wiederverwendung der vorhandenen Dinge“ (Siehe Kevin Kelly „Unvermeidlich“, übersetzt von

Auswirkungen auf die aktuellen gesetzlichen Regeln, die Rechtsstruktur und die ethischen Standards. Es zeigt nicht nur die Mängel in der aktuellen Versorgung mit Produkten des Rechtssystems auf, sondern stürzt sogar auch das etablierte Rechtsverständnis der Menschen um. Daher ist es im Zeitalter der Neuvermischung eine wichtige Voraussetzung, um die rechtlichen Grundprinzipien, institutionellen Regeln und ethischen Normen festzulegen, mittels dessen, das Wesen der sozialen Struktur zu erfassen, das Modell der sozialen Beziehungen zu rekonstruieren und die menschliche Natur als Grundlage des Gesetzes zu erläutern. Die Menschheit tritt in ein neues Zeitalter ein, in dem sie ihre Gesetze neu aufbauen muss, um die virtuelle Welt zu regulieren, da der traditionelle Mechanismus zur Generierung von Gesetzen die Anforderungen der Legalisierung der virtuellen Welt nicht mehr erfüllen kann. Das ist eine Ära, in der sich die Regelsysteme der virtuellen Welt und die Rechtssysteme der realen Welt aneinander anpassen und Gesetze in verschiedenen Formen geschaffen und reformiert werden. Die digitale Zivilisation liefert die Motivation für Innovationen zur Einrichtung des Datenrechtsgesetzes, während das Datenrechtsgesetz die existenzielle Grundlage für Verbesserung der Ordnung der digitalen Zivilisation bildet. Während sich die menschliche Gesellschaft von der landwirtschaftlichen zur industriellen Zivilisation und dann zur digitalen Zivilisation entwickelt, wird das Gesetz vom „Gesetz der Menschen“ zum „Gesetz der Dinge“ und dann zum „Gesetz der Daten“ überspringen.

(I) Persönlichkeit der Datenperson

Wir befinden uns in einer Welt, die von Datenpersonen umgeben ist. Wir können ihnen nicht die Augen verschließen, wenn sie in der Neuzeit in das Lebensfeld der modernen Menschlichkeit eintreten. Das 21.

Zhou Feng et al. Verlag der Elektron-Industrie, 2016, S. 240). Die Neuvermischung beinhaltet interne Struktur und Bewegungsprozess, in denen Chaos und Ordnung koexistieren, im Gegensatz zueinander stehen und gegenseitig wechseln. Es ist nicht die starre Mischung aus alten und neuen Methoden, sondern die Rekonstruktion von Modi für die Integration und Anordnung von Komponenten.

Jahrhundert ist ein digitales, vernetztes und intelligentes Zeitalter. Die Datenmacht und die Datenbeziehungen in diesem Zeitalter erfordern zwangsläufig, dass sich die Rechtsgrundsätze und das Rechtssystem von denen unterscheiden, die im 19. Jahrhundert auf die Fließbänder und im 20. Jahrhundert auf die Automatisierung als Regulierungsobjekt abzielen. Das traditionelle Rechtssystem, insbesondere das System der Rechtssubjekte, war oder ist mit beispielloser Herausforderungen konfrontiert. Die wissenschaftlichen und technologischen Fortschritte verändern unser Verständnis des Gesetzes und führen zur Rekonstruktion unserer gesetzlichen Regeln. Es zwingt uns wiederum, unser Persönlichkeitssystem auf der Grundlage der sozialen Realität und aus der Perspektive der Rechtstheorie zu überprüfen⁸ und darüber nachzudenken, ob es notwendig ist, der Datenperson Rechtspersönlichkeit zu verleihen. Gesetzliche Rechte müssen auf der Persönlichkeit beruhen, sonst würden sie im Widerspruch zur sozialen Wohlfahrt stehen (Robert Morrison MacIver 1946, S. 180). Die Studie über die Gründe, warum die Datenperson Rechtspersönlichkeit haben soll, ist tatsächlich der Kerninhalt zukünftiger Anpassungen des Gesetzes. Mit zunehmender Sozialisierung der Datenperson ist es notwendig, ihren rechtlichen Status zu untersuchen, um die Lücke zwischen der sozialen Entwicklung und dem Gesetz zu schließen.⁹ David

- 8 Persönlichkeit bezieht sich im Allgemeinen auf die fachliche Qualifikation, die der als Mensch geborene und lebende Mensch besitzt und den Menschen von anderen Arten und Formen unterscheidet. Sie ist vor allem ein philosophischer Begriff. Später wurde der Begriff der Persönlichkeit in der Rechtstheorie nach mehrmaliger Evolution und Erweiterung schließlich als das gesetzlich anerkannte und dem Menschen innewohnende Interesse an der Persönlichkeit bestimmt. Das heißt, Persönlichkeit ist die Qualifikation des Menschen, unabhängig und würdevoll Rechte zu genießen, Pflichten zu übernehmen und persönliche Freiheit zu erlangen und erzeugt so verschiedene spezifische Persönlichkeitsrechte. Sie ist die Grundlage und Voraussetzung für den Menschen, andere Bürgerrechte zu genießen und zivilrechtliche Handlungen durchzuführen.
- 9 Der vom Staatsrat veröffentlichte „Entwicklungsplan für künstliche Intelligenz der neuen Generation“ weist auf die Notwendigkeit hin, relevante rechtliche Fragen zu untersuchen und ein System der Rechenschaftspflicht einzurichten und macht es eindeutig zum strategischen Ziel, „ein System von Gesetzen und Vorschriften für künstliche Intelligenz und ethische Normen sowie politische Richtlinien

C. Vladeck, Professor für Recht an der Georgetown Law School, führte am Beispiel von Personenschädigung durch ein unbemanntes Fahrzeug die Fragen an, wie unsere Gesetze mit Robotern umgehen sollen und wie die Haftung für Folgen ihres Verhaltens zugeteilt werden soll. Ihm zufolge ist der rechtliche Status von Robotern ein Thema, mit dem sich die Gesetzgebung befassen muss (David C. Vladeck 2014). Mit der Entwicklung intelligenter Roboter müssen unsere Verfassung und Gesetze möglicherweise geändert oder neu geschrieben werden (Phil McNally & Sohail Inayatullah, 1988).

Gegenwärtig schreitet die Technologie mit exponentieller Geschwindigkeit voran. Die Zukunft ist voller enormen Unsicherheiten und Risiken. Die Menschheit muss wachsam davor sein. Martin Heidegger wies in seinem Buch „The Question Concerning Technology“ darauf hin, dass moderne Technologie nicht mehr neutral sei und als „Gestell“ [wörtlich „Enframing“] das ganze Leben des modernen Menschen kontrollierte und beherrschte, oder zum historischen Schicksal des modernen Menschen geworden sei. Die Entwicklung der Biotechnologie und der intelligenten Technologie verändert den „Menschen“ im Wesentlichen, der Mensch wird repariert, transformiert und seine Elemente werden

aufzustellen“, wobei er auch vorschlägt, „Gesetze, Vorschriften und ethische Normen zur Förderung der Entwicklung künstlicher Intelligenz zu formulieren“, um die gesunde und rasche Entwicklung künstlicher Intelligenz zu gewährleisten. Darüber hinaus wurde insbesondere auf die Notwendigkeit hingewiesen, sich aktiv an der globalen Steuerung der künstlichen Intelligenz zu beteiligen, das Studium über Fragen der künstlichen Intelligenz mit wichtiger internationaler Gemeinsamkeit wie Entfremdung und Sicherheitskontrolle von Robotern zu intensivieren und die internationale Zusammenarbeit in Bereichen Gesetze, Vorschriften und Internationale Regeln für künstliche Intelligenz zu vertiefen, gemeinsam die globalen Herausforderungen zu bewältigen und die Allokation von Innovationsressourcen auf globaler Ebene zu optimieren. Es ist unerlässlich, sich an international anerkannte Praktiken anzupassen und am globalen Dialog über die Spezifikationen, Standards und Spezifizierungsmethoden für die Entwicklung künstlicher Intelligenz teilzunehmen, die Studie über Gesetze und Vorschriften in Bezug auf künstliche Intelligenz zu verbessern und die Rechte, Pflichten und Verantwortlichkeiten in Bezug auf künstliche Intelligenz klarzumachen, wobei die Studie über den rechtlichen Status der künstlichen Intelligenz als Schwerpunkt und Kern genommen werden soll.

neu kombiniert. Mensch-Maschine-Interdependenz, Mensch-Maschine-Interaktion, Mensch-Maschine-Kombination, Mensch-Maschine-Synergie und Mensch-Maschine-Integration werden zum allgemeinen Trend. Der amerikanische Futurist Ray Kurzweil behauptete, dass „die biologische Intelligenz mit der nichtbiologischen Intelligenz, die wir schaffen, unvermeidlich eng verbunden werden müssen“ (Ray Kurzweil 2015). Wenn Mensch und Maschine zunehmend symbiotisch oder integriert werden, stellt sich die Frage, ob dieser Symbiont ein „Mensch“ oder eine „Maschine“ sein soll? Wahrscheinlich gibt es keine endgültige Antwort auf diese Frage. Wäre die Datenperson in gewissem Sinne ein „Mensch“, hätte sie Grundrechte wie Menschenrechte etc.? Und besäße sie wie ein natürlicher Mensch Persönlichkeit und Würde? Sollte sie als Subjekt für Rechtsbeziehungen und moralische Beziehungen identifiziert werden und entsprechende Konsequenzen ihrer Verhaltensweise tragen? Es gibt viele solche Fragen und es tauchen stets neue Fragen auf. „Wir sollen jetzt sofort mit einer echten Diskussion beginnen: Was ist unsere Identität im Vergleich mit diesen Maschinen?“ (John Jordan 2018, S. 162). Es ist ein neues Verständnis erforderlich, was der „Mensch“ ist, was das Wesen des Menschen ist und welche Wertprinzipien beim Umgang mit zwischenmenschlichen Beziehungen und Mensch-Maschine-Beziehungen zu beachten sind (Sun Weiping 2017). Ray Kurzweil sagte sogar voraus, dass Roboter mit Selbstbewusstsein im Jahr 2029 auftauchen und in den 30er-Jahren des 21. Jahrhunderts ganz allgemein werden. Sie werden verschiedene subtile Emotionen haben, die denen des Menschen ähnlich sind (Ray Kurzweil 2014, S. 195). Es erscheint uns unangemessen, eine solche Datenperson als Roboter zu betrachten, da sie sich nicht mehr wie Maschine anfühlt. Da Diskussionen über die Rechtspersönlichkeit der Datenperson eine wichtige theoretische Bedeutung und einen wichtigen praktischen Wert haben, hat die Wissenschaftswelt Ideen wie E-Persönlichkeit, virtuelle Persönlichkeit und eingeschränkte Persönlichkeit vorgestellt. Es muss angemerkt werden, dass relevante Forschung „den notwendigen Systemraum für das Wachstum neuer Technologien reservieren sollte“ (Wang Liming 2018).

Obwohl diese nur Postulierungen sind, soll die Menschheit wahrscheinlich Vorsichtsmaßnahmen treffen und dieses letzte wichtige

Rechtsproblem der Menschheit mit Vorsicht behandeln.¹⁰ Bei der Analyse der Bedeutung der Rechtspersönlichkeit stellte Hoshino Echi, ein japanischer Ziviljurist, fest, dass „sogar andere Wesen als Menschen anerkannt werden könnten, wenn sie als ein Begriff des Hauptträgers für privatrechtliche Rechte und Pflichten geeignet sind“ (Hoshino Echi 2004, S. 21). Der israelische Historiker Yuval Noah Harari war der Meinung, dass „der vom Gesetz der Menschheit anerkannte Hauptträger der Intersubjektivität von Unternehmen oder Nation als „juristische Person“ bezeichnet ist. Obwohl ‚Toyota‘ oder ‚Argentinien‘ weder Körper noch Seele haben, sind beide jedoch an das Völkerrecht gebunden, können Land und Geld besitzen und Kläger oder Angeklagter vor Gericht werden könnten. Der Algorithmus könnte wahrscheinlich auch bald danach einen solchen Status erhalten“ (Yuval Noah Harari 2017, S. 293). Während im akademischen Kreis eine hitzige Debatte stattfindet, bleibt der Gesetzgeber nicht zurück und tritt ebenfalls in den Vordergrund. Im Jahr 2017 schlug der Rechtsausschuss des Europäischen Parlaments vor, „langfristig einen spezifischen Rechtsstatus für intelligente Roboter zu schaffen, damit zumindest die ausgereiftesten autonomen Roboter den Status elektronischer Person haben, die Verantwortlichkeit für Beseitigung der von ihnen verursachten Schäden tragen sollen. Dies kann dazu führen, dass Roboter autonome Entscheidungen treffen oder auf andere Weise unabhängig mit Dritten interagieren und dabei möglicherweise die elektronische Persönlichkeit anwenden“ (siehe Rechtsausschuss des Europäischen Parlaments 2015). Nachfolgend schlug Russland in Artikel 1 des Grishin-Gesetzes vor, Robotern den rechtlichen Status eines „Roboteragenten“ zu gewähren und erklärte, dass ein Roboteragent sein unabhängiges Eigentum besitzen und die Haftung für seine eigenen Schulden mit diesem Eigentum übernehmen soll und dass er Bürgerrechte erhalten und ausüben kann und zivilrechtliche Verpflichtungen im eigenen Namen eingehen (Zhang Jianwen 2018). Weltweit

10 Stephen Hawking, berühmter Physiker, erklärte einmal, dass „der Erfolg bei der Schaffung künstlicher Intelligenz das größte Ereignis in der Geschichte der menschlichen Zivilisation und auch das letzte Ereignis sein könnte“ und „die Entwicklung künstlicher Intelligenz das Ende der Menschheit bedeuten könnte.“ Siehe Sun Weiping: „Reflektion zum Wert der künstlicher Intelligenz“, „Philosophische Forschung“, 2017, 10. Ausgabe.

akzeptieren Länder den subjektiven Status der Datenperson hauptsächlich auf zwei Arten. Einige Länder wenden Gesetzgebung an. Saudi-Arabien zum Beispiel verleiht dem Roboter „Sophia“ die Staatsangehörigkeit von Saudi-Arabien durch Gesetzgebung. In anderen Ländern, in denen zu diesem Zweck keine Rechtsvorschriften für klare Festlegung des subjektiven Status der Datenperson vorhanden sind, werden aber Richtlinien erlassen, um die Entwicklung von Robotern zu unterstützen und Robotern einen entsprechenden Rechtsstatus zu gewähren. Bisher hat China Datenperson auf keine dieser Arten einen Rechtsstatus eingeräumt, und der Hauptträger von Straftaten bleibt im Prinzip natürliche Person, die das Alter für die strafrechtliche Verantwortlichkeit erreicht haben und die Fähigkeit zur strafrechtlichen Verantwortlichkeit besitzen. Zum Beispiel sieht Artikel 2 der „Allgemeinen Bestimmungen des Zivilrechts“ vor, dass „das Zivilrecht die persönlichen Beziehungen und Eigentumsverhältnisse zwischen den gleichberechtigten Hauptträgern wie der natürlichen Personen, juristischen Personen und nicht juristischen Körperschaften regelt“.¹¹

Die Struktur des Rechtssystems ändert sich seit jeher ständig. Die Komplexität der sozialen Entwicklung wird auf die Unterschiede in Bezug auf Rechtspersönlichkeit, Status, Identität, Rechte, Qualifikationen und Verantwortlichkeiten zurückgeführt, die nach dem Gesetz verschiedenen Subjekten übertragen worden sind. Der erweiterte Umfang der Rechtssubjekte spiegelt die dynamischen Veränderungen in der Grundidee und im Wert des Gesetzes wider. Was den Evolutionsprozess des Gesetzes betrifft, so scheinen wir keinen Grund zu haben, daran zu zweifeln, dass der Geltungsbereich der Rechtssubjekte künftig auf Datenpersonen oder andere neue Arten im Cyberspace ausgedehnt werden könnte, und dies ist nichts anderes als sie nach dem Bedürfnis des Rechtssystems und des Sozialsystems erstellt worden sind. In der Geschichte der Konstruktion des Begriffs des Rechtssubjekts brechen die Rechtsstreitigkeiten in Bezug auf die Sklavenbefreiung, die Bewegung für gleiche Rechte, den Feminismus,

11 Obwohl juristische und nicht juristische Personen keine natürlichen Personen sind, können sie nicht unabhängig von den „personifizierten“ Einheiten natürlicher Personen sein und so haben sie immer noch die Eigenschaften natürlicher Personen.

die Arbeitsorganisationen, Körperschaftssystem und in Bezug auf Embryonen, Personen im vegetativen Zustand und geneditierte Babys sowie einschließlich der neuen Typen von Rechtsansprüchen aus Rechtsstreitigkeiten und Sammelklagen von öffentlichen Interessen die moderne Theorie zu Rechtssubjekt kontinuierlich durch. Dies zeigt, dass sich der Begriff der Rechtspersönlichkeit mit der Zeit weiterentwickelt und flexibel ist (Yu Chengfeng 2017). Das Rechtssubjekt hat Veränderungen von „Mensch als Nichtmensch“ bis „Nichtmensch als Mensch“ zu behandeln erfahren. Dies verkörpert den Prozesstrend in Richtung der schrittweisen Offenheit der Spezifikation des Rechtssubjekts.¹² Genau wie Maus, religiöse Heterodoxie und Hexe, die zu bestimmten Zeitpunkten in der Geschichte als Angeklagte vor Gericht gebracht wurden, wird Datenperson in Zukunft wahrscheinlich

- 12 Beispielsweise hat das US-Bundesgericht ein im Namen des Byram River eingereichtes Verfahren gegen ein Unternehmen an Land eingeleitet, weil es Umweltverschmutzung verursacht hat. Die Sierra Club Law Protection Foundation und die Hawaii Audubon Society reichten einmal eine Beschwerde im Namen von Palila ein, einer Vogelart, von der nur noch wenige hundert übrig waren. Richter Williams Douglas erklärte in seiner Arbeit: „Sollten Bäume stehen? Auf dem Weg zu gesetzlichen Rechten für natürliche Objekte“, die Nationen, Unternehmen, Säuglingen, Personen ohne Verhaltensfähigkeit, autonomen Städten und Universitäten usw., die nicht sprechen oder kein Bewusstsein haben und ihnen Beschützer oder Agenten zugewiesen oder gesetzliche Rechte verliehen werden können; warum kann das Gesetz natürlichen Objekten keine rechtliche Stellung verleihen? Eine alte Frau in Italien hinterließ ein Testament und schenkte ihrem Lieblingshund 50 Prozent ihres Eigentums, d.h. eines Nachlasses im Wert von mehr als 1 Million Euro, und machte dadurch diesen zum ersten Hund im Wert von mehr als 1 Million Euro in der italienischen Geschichte. Ähnliche Beispiele waren der Schäferhund Gunther IV im Wert von 224,6 Mio. GBP, der Schimpanse Luka im Wert von 53 Mio. GBP und die Katze Tomasio im Wert von 15,66 Mio. USD. Alle diese Beispiele veranschaulichen, dass Subjekte in zivilen Beziehungen nicht mehr auf natürliche Personen beschränkt sind und viele Objekte, die keine natürlichen Personen sind, basierend auf den Bedürfnissen der Gesetzgeber nach und nach als juristische Person akzeptiert werden und den Status von Subjekten in zivilen Beziehungen erhalten und dies zeigt einen wachsenden Trend, „Nichtmensch als Mensch zu behandeln“. Dies hat auch Interpretationsspielraum für Gewährung des zivilrechtlichen Rechtsstatus für solche Humanoide wie Datenperson geschaffen.

auch als Angeklagte, Kläger oder sogar Richter, Anwalt oder Notar in der Zukunft eine Rolle bei den neuen Regeln spielen. Mit der Begründung, dass Tiere immer noch bestimmte Rechte haben, forderten einige Menschen, dass die Datenperson respektiert werden soll, da sie Bewusstsein und Gefühl hat und es immer schwieriger wird, zwischen Datenpersonen und natürlichen Menschen zu unterscheiden. Wie der französische Denker der Aufklärung, Jean-Jacques Rousseau, im „Diskurs über den Ursprung und die Grundlage der Ungleichheit unter den Menschen“ feststellte, sollten Tiere die von der Natur eingeräumten Rechte genießen, und die Menschheit ist auch verpflichtet, diese Rechte aufrechtzuerhalten. Jeremy Bentham, der Begründer des Utilitarismus, gehörte zu den Befürwortern der Tierrechte. Im Manuskript einer Rede über die Notwendigkeit, die gesetzlichen Rechte von Tieren zu erweitern, schrieb er: „Der Tag wird endlich kommen, an dem der Rest der Tierkreation jene Rechte erwerben kann, die ihnen nur durch die Hand der Tyrannei hätten vorenthalten werden können und diese Rechte sollen seit jeher nicht beraubt werden.“ In Bezug auf Ansprüche auf Tierrechte können wir vielleicht die Rechtmäßigkeit von Rechten für Datenperson ableiten.

In Zukunft wird der Umfang der Gesetzsubjekte wahrscheinlich über die Grenzen des „Menschen“ im biologischen Sinne hinausgehen und die Spezies sind möglicherweise nicht das Haupthindernis für die Gewährung von Rechten. Rechtssysteme sollen der Evolutionslogik der Rechtssubjekte folgen. „Es sollte eine offene Haltung gegenüber dem Status von Robotern als Rechtssubjekt entwickelt werden und es sollte auch gelehrt werden, dass Artenunterschiede eine technische Schwierigkeit für die gesetzlichen Rechte darstellen“ (Zhang Yujie 2017). In Zukunft wird die Rechtsordnung sehr wahrscheinlich einen neuen Persönlichkeitsrang für die Teilnahme an Rechtsprozessen machen, indem verschiedene Arten von Rechtspersönlichkeitsmasken erstellt werden, damit sowohl Datenperson als auch „andere Personen“ alle einen „Knoten im Bündel von Rechten“ in Rechtsbeziehungen einnehmen und als verteilte Knotenpunkte in Rechtsbeziehungen in der künftigen gesetzgeberischen Betrachtung und Rechtspraxis fungieren können. „Obwohl es große Auswirkungen auf den alten legalen Dogmatismus haben mag, spielt es jedoch positive Funktionen, die zur Anpassung an die soziale Entwicklung beitragen“ (Zhou Xiang 2019).

Die Entwicklung von Datenpersonen ist unvermeidlich und es sind auch gesetzliche Regeln erforderlich, die die Entwicklung von Datenpersonen regeln. Die Regulierung von Datenpersonen beruht auf Anpassungen des Rechtssystems und der institutionellen Regelungen des Gesetzes, die die diesbezügliche Entwicklung in einem angemessenen Rahmen halten. Alles, was oben geschildert ist, weist darauf hin, dass es an der Zeit ist, Datenrechte und Datenpersonen angemessen zu regeln und die Ordnung der relevanten Gesetze und moralischen Standards festzulegen und zu verbessern.

(II) Institutionelles System der Datenrechte

Die Menschheit macht immer notwendige institutionelle Entwürfe basierend auf ihren eigenen Bedürfnissen als Mittelpunkt. Das institutionelle System der Datenrechte ist eine wichtige Grundlage und ein wichtiges Prinzip für den Schutz der Rechte und Interessen der Datenressourcen. Daher ist es unerlässlich, ein institutionelles System und eine Reihe von Betriebsregeln für Datenrechte zu errichten. Bisher gibt es noch keine „einheitliche Theorie“ zum „Datenrechtssystem“ sowohl im theoretischen als auch im praktischen Kreis und in einigen spezifischen Fragen bestehen weiterhin Meinungsverschiedenheiten. Dennoch ist den Menschen klar bewusst, dass das bestehende Rechtssystem für Datenrechte Probleme hinsichtlich seiner theoretischen Grundlage, Struktur, Anwendung in der Praxis und anderer Aspekte aufweist und dass „kleine Änderung und Überarbeitung“ nicht ausreichen, um seine Mängel und Schwachstellen wettzumachen. Vor dem Hintergrund, dass eine neue Runde der technologischen Revolution und des industriellen Wandels im Gange ist, wurden neue Anstrengungen im Ausland schon unternommen, um die Gesetze zum Datenschutzsystem zu ändern. Wir sollen Acht auf Untersuchung des Gesamtdesigns des Datenrechtssystems geben. Dies liegt daran, dass die Analyse bestimmter Arten von Datenrechten, egal wie sorgfältig und detailliert sie auch sind, letztendlich nur empfindliche Komponenten hervorbringen würde, die aber nicht zusammengesetzt werden könnten. Deshalb müssen wir erwägen, ein institutionelles Datenrechtssystem zu schaffen, das dem Trend der modernen sozialen

Entwicklung entspricht. In der heutigen Gesellschaft erfordert die chaotische Unordnung und das Fehlen von Regeln in Datenrechtsbeziehungen unmittelbar die Einrichtung eines soliden Datenrechtssystems. Die klare Trennung zwischen der Zugehörigkeit der Datenrechte und der Verwendung von Daten ist der Hauptgrund für die Einrichtung eines Systems zur Datenteilhabe, während der gegenseitige Nutzen die realistische Grundlage für das eigenständige System zur Datenteilhabe darstellt.

Das Rechtssystem koordiniert zwischen dem Ideal und der Realität der Gesellschaft oder, anders ausgedrückt, es gehört zur Grauzone zwischen der Standardwelt und der realen Welt. Dies gilt insbesondere für das Datenrechtssystem. Ihre Bedeutung liegt nicht nur in der Wahrung und Aktualisierung der Gerechtigkeit, sondern auch in der Bemühung für Schaffung von Ordnung, d.h. der Minimierung der Datentransaktionskosten und der Verbesserung der Effizienz der Zuweisung von Datenressourcen mit institutionellen Vereinbarungen, die die Beziehungen und Regeln der Datenrechte kombinieren und die Datenrechtsbeziehungen effektiv integrieren, anpassen und schützen. Zu diesem Zweck müssen wir ein ganzes institutionelles System schaffen, das sich auf Datenrechte konzentriert. Der erste Teil davon ist das System der Legalisierung von Datenrechten. Dieses System enthält gesetzliche Bestimmungen und Beschreibungen unter anderem in Bezug auf die Konnotation, Epitaxie, das Realisierungsverfahren, den Vernichtungsprozess und die Hilfsmittel usw., indem sie ein System einrichtet, das die Rechtsgrundlage für die Realisierung von Datenrechten schafft. Die Einrichtung eines Systems zur Legalisierung von Datenrechten kann zur Umwandlung von ordnungsgemäßen Datenrechten in gesetzliche Datenrechte und reale Datenrechte beitragen. Datenrechte stellen eines der Grundrechte für das Überleben und die Entwicklung der Menschheit dar und sollen zu gesetzlichen Datenrechten gesteigert werden. Und die Datenrechte an sich sollen gerechtfertigte und angemessene Interessenansprüche darstellen und den realistischen Anforderungen der relevanten Systeme und der Wertorientierung entsprechen. Der zweite Teil dieses Systems ist das Dateneigentumssystem. Das Dateneigentum, das die vollständigste Vorherrschaft über Daten gewährt und bildet den Kern des Datenrechtssystems. Es umfasst vor allem die Rechte zu Steuerung, Verwendung, Verdienst und Teilhabe von Daten, während diese vier

Funktionen unter bestimmten Bedingungen getrennt werden können. Das Dateneigentumssystem bedeutet eine Zugehörigkeitsform, in der die Daten zu einem bestimmten Eigentümer auf institutioneller Ebene zugewiesen werden und die Daten unter der vollständigen Kontrolle des Eigentümers stehen. Das Dateneigentumssystem durchbricht die Einschränkung der traditionellen Idee, dass „Dinge Körper haben müssen“ und mildert gleichzeitig die geschlossene und exklusive Struktur des traditionellen Eigentums und das Prinzip „ein Eigentum für ein Objekt“. Auf diese Weise ist es hilfreich sowohl dafür, die Rechte und Interessen der Inhaber von Datenrechten zu schützen, als auch die Teilhabe und Verwendung von Daten in der gesamten Gesellschaft zu fördern. Das dritte ist das System des Nießbrauchsrechts von Daten. Die Nießbrauchrechte an Daten werden generiert, um den Konflikt zwischen dem Eigentum an und der Nachfrage nach Daten zu lösen. Sie sind unter bestimmten Bedingungen Rechte auf Nutzung von und das Recht auf Erträge aus Daten, die anderen Personen gehören. Die Nießbrauchrechte von Daten ist eine Art Fremddatenrechte und auch eine Art von eingeschränktem Dateneigentumsrecht. Die Nießbrauchrechte von Daten beinhalten die Verfügung des Nutzungswerts von Daten und können drei Funktionen abdecken, nämlich das Kontrollrecht, das Nutzungsrecht und das Verdienstrecht. Das System der Nießbrauchrechte von Daten ist das Ergebnis des Übergangs von dominanzzentrierten Datenrechten zu nutzungszentrierten Datenrechten. Es kann uns helfen, den Wert von Datenrechten besser zu erkennen und dient als Methode zur Aktualisierung des Eigentumsrechts. Das vierte ist das System der Nießbrauchrechte auf öffentliche Daten. Die Nießbrauchrechte auf öffentliche Daten beziehen sich auf alle Rechte, die den öffentlichen Rechten entsprechen und die von den Verwaltungsinstitutionen zu den von ihnen bereitgestellten oder verwalteten gemeinnützigen Daten festgelegt werden, um das Gemeinwohl zu gewährleisten und zu verbessern. Es handelt sich um eine Art übertragene „Nießbrauch-Datenrechte“. Das Objekt ist öffentliche Daten und das Subjekt sind Verwaltungsinstitutionen wie die Regierung und breite Öffentlichkeit usw. Für die von der Regierung vertretenen Verwaltungssubjekte umfassen die Nießbrauchrechte für öffentliche Daten das Recht zur Datenerfassung, das Recht zur Planung der Datenentwicklung, das Recht zur Erteilung der Erlaubnis zur Nutzung von Daten usw.

Für die breite Öffentlichkeit gehören das Recht auf informierte Zustimmung zu Daten, das Recht auf Datenänderung, das Recht auf Vergessen von Daten usw. zu den Rechtsarten des Nießbrauchsrechts für öffentliche Daten. Das fünfte ist das Teilhabesystem. Das Datenrecht ist in der Natur das Teilhaberecht. Das zentrale Anliegen des Teilhaberechtssystems ist das Gleichgewicht zwischen den Datenrechten und -interessen von Einzelpersonen und den öffentlichen Interessen an Daten. Das Teilhabesystem korrigiert die ehemalige Datenansicht „Bevorzugung privater Interessen gegenüber öffentlichen Interessen“ und schlägt stattdessen einen neuen Ansatz vor und befürwortet die Datenanschauung, die ein Gleichgewicht zwischen privaten Interessen und öffentlichen Interessen anstrebt. Das Gleichgewicht zwischen den persönlichen Datenrechten und -interessen und den öffentlichen Interessen ist mittlerweile auch das grundlegende Problem von Innovationen und Regelungen im Datenrechtssystem. Das Teilhabesystem mit einer gerechten Verteilung privater und öffentlicher Interessen als Kernprinzip bietet eine wertvolle Grundlage für Lösung der Konflikte zwischen verschiedenen Interessengruppen und Datenrechtshabern. Diese fünf Hauptdimensionen bilden das Schutzsystem für personenbezogene Daten, das für die Wertziele der bestmöglichen Nutzung von Daten und Gewährleistung der Datensicherheit usw. eingerichtet wurde. Der Schutz personenbezogener Daten soll jedoch nicht nur den Schutz persönlicher Rechte umfassen. Es soll über die „Zustimmung“ oder „Informiert-Werden“ hinausgehen und eine offene, integrative und freundliche Haltung gegenüber der industriellen Entwicklung und sozialen Gerechtigkeit einnehmen, die Dynamik und Flexibilität der einschlägigen Regeln beibehalten und durch bessere (und nicht mehrere) Nutzung des Mechanismus der „von unten nach oben“ und verteilten Regelgenerierung eine Reihe von Unterstützungssystemen, die den spezifischen Wertzielen besser dienen, einrichten, um ein Datenschutzsystem zustande zu bringen, das die praktischen Anforderungen besser erfüllen.

Derzeit fallen die Fragen zu Datenrechten hauptsächlich in zwei Kategorien: Eigentum und Nutzung. Dementsprechend kann der Rahmen des Datenrechtssystems grundsätzlich aus zwei Teilen wie dem System der Datenrechtzugehörigkeit und dem System der Datennutzung bestehen. Es geht nicht nur einfach darum, das Rechtssystem für die Datennutzung zu

vereinheitlichen, sondern um eine Reform der traditionellen Wertansicht. Auf dem von uns geplanten logischen Gedankenweg wird man definitiv einen neuen Ansatz in Bezug auf Datenrechte und neue Ethik erreichen und unweigerlich neuen Betriebsmechanismus für Datenrechte generieren. „Nach den Grundprinzipien des Aufbaus von Rechtssystemen wird die Kombination von Rechtsnormen immer durch die Konzepte spezifischer Systeme eingeschränkt. Unterschiedliche Rechtsnormen müssen koordiniert und komplementär sein und dürfen keine Konflikte und Widersprüche aufweisen“ (Xia Xiaoxiong 2019). Das ist ein wichtiger Punkt beim Aufbau des institutionellen Systems der Datenrechte. Für Gesetzgeber haben das Konzept der Funktionalität, das allgemeine Prinzip und die typisierte Strukturierung für Aufbau der Struktur des Datenrechtssystems wichtige Bedeutung. Auf der Grundlage einer systematischen Transformation sollen daher „Instrumente“ wie das Konzept der Funktionalität, grundsätzliche Spezifikationen, die typisierte Unterscheidung usw. effektiv angewendet werden, um das Datenrechtssystem zu konstruieren, ordnungsgemäß anzuordnen und die interne Logik und Systemzusammenhang im Bereich der Datenrechtsnormen zu optimieren.

Obwohl die aktuelle Studie noch nicht ausreicht, um einen konkreten Vorschlag für ein ausgereiftes Datenrechtssystem zu unterbreiten, hat sie aber eine glänzende Zukunft und können definitiv zum Aufbau des Datenrechtssystems beitragen. Da es heute häufig und in großer Zahl zu Streitigkeiten über Datenrechte kommt, müssen unter anderem die Art, der Status und Inhalt des Dateneigentums¹³, Datenrechte¹⁴,

13 Die Datenrechtsaffirmation ist der logische Ausgangspunkt für den Schutz von Datenrechten und die Voraussetzung für Festlegung von Datenregeln. Die Eigentümerschaft ist für Daten unterschiedlicher Art oder in unterschiedlichen Phasen ihres Lebenszyklus auch unterschiedlich. Datengrenzen, einschließlich der Grenze offener Regierungsdaten, der Grenze der kommerziellen Nutzung von Unternehmensdaten und der Grenze des Privatsphäreschutzes personenbezogener Daten, sollten durch die Gesetzgebung klar definiert werden.

14 Datenrechte sind ein wichtiger Bestandteil der Datenrechtsgesetzgebung. Und ein Gesetz, das nichts mit Rechten zu tun hat, wird wahrscheinlich kein Interesse daran wecken. Die Gesetzgebung soll Datensubjekten Rechte wie das Recht auf Datenzugriff auf Daten, das Recht auf Berichtigung von Daten, das Recht auf Vergessen von Daten, das Recht auf Datentragbarkeit, das Recht auf Nutzung

Datennutzung¹⁵ und Datenschutz¹⁶ angegeben werden. Darüber hinaus gibt es realistische Materialien für relevante Analyse, Studie und Reflexion. In China wurden eingehende Untersuchungen und Diskussionen über das Datenrechtssystem aus verschiedenen Perspektiven und auf verschiedenen Ebenen in allen Kreisen der Gesellschaft durchgeführt. Auf der Ebene der Gesetzgebung finden sich zerstreut relevante Bestimmungen in den Branchengesetzen, aber keines dieser Gesetze trägt den Datenschutz in seinem Namen. Wenn Daten als eine Art grundlegende strategische Ressourcen des Landes betrachtet werden, müssen noch mehr Anstrengungen unternommen werden, um allgemeine Überlegungen für das System anzustellen und ein umfassendes strategisches Design zu erstellen. Die Modernisierung des Rechtssystems für Datenrechte

von Daten, Erlöserecht aus Daten und das Recht zur Datenentlastung usw. einräumen. Es soll nicht nur Bestimmungen über die Rechte von Dateneigentümern wie das Recht auf Kontrolle von Daten, das Recht auf Nutzung von Daten und das Recht auf Ertrag aus Daten enthalten, sondern auch Bestimmungen über das Recht anderer auf Nutzung von Daten wie die Nießbrauchrechte von Daten, die Nießbrauchrechte öffentlicher Daten und das Recht auf Datenteilhabe etc.

- 15 Der Wert von Daten liegt in ihrer Verwendung. In Haltung am Prinzip der bestmöglichen Nutzung von Daten wird der Wert von Daten durch kommerzielle, administrative und zivile Nutzung erschlossen und die Geburt des Modells der Datennutzung, d.h. die „drei Ketten-Kombination“, nämlich die gesamte Industriekette und die gesamte Verwaltungskette und die gesamte Servicekette gefördert wird. Das Ziel der Regulierung der Datenrechte liegt darin, die öffentlichen Interessen und die öffentliche Sicherheit zu schützen und gleichzeitig die freie Teilhabe an personenbezogenen Daten zu fördern. Zu diesem Zweck müssen die Bürger einen Teil ihrer Datenrechte übertragen. Die Gesetzgebung soll anstreben, spezifische Kriterien für Realisierung des Gleichgewichts zwischen Rechtsschutz und angemessener Verwendung von Daten festzusetzen.
- 16 Die Verantwortung für den Schutz bildet einen unentbehrlichen wichtigen Bestandteil von Gesetzen, Vorschriften und Regeln. Wenn ein Gesetz keine Bestimmungen zur Schutzverantwortung enthält, sind die darin vorgesehenen Rechte und Pflichten nutzlos. Für Aspekte wie die Datenerfassung, -speicherung, -übertragung und -nutzung etc. ist eine intensivierete Sicherheitskontrolle erforderlich, um Angriffe auf Daten sowie Datenlecks, Diebstahl, Manipulationen und illegale Nutzung von Daten zu verhindern. Außerdem geht es bei Daten um die staatliche Sicherheit und nationalen Interessen, und ein separater Schutz der Datensouveränität auf nationaler Ebene ist erforderlich.

ist keineswegs eine partielle Verbesserung eines Systems oder in einigen einzelnen Aspekten. Im Grunde genommen erfordert es ganzheitliche Anpassungen des Datenrechtssystems, damit verschiedene Systeme und verschiedene Aspekte ausgewogen synergetische Wirkung generieren, die sowohl der internen Systemlogik entsprechen als auch zur Anpassung an die externen praktischen Anforderungen koordiniert werden können. Außerdem sollen aktive Anstrengungen unternommen werden, um die Früchte der Entwicklung der legalen Zivilisation der Menschheit aufzunehmen und die nützlichen Erfahrungen, Elemente und Mechanismen usw. ausländischer Datenrechtssysteme als Beispiel rational zu nutzen, damit das Datenrechtssystem zu einem wichtigen Bestandteil des Rechtssystems unter neuen historischen Bedingungen werden kann.

(III) Moderation der Legalisierung von Datenrechten

Das Prinzip der Legalisierung von Datenrechten ist als „eine der wichtigen Säulen der Strukturierung des Sachenrechtsgesetzes“ angesehen (Xie Zaiquan 1999, S. 40). Wie die Gesetze in vielen anderen Bereichen muss auch das Datenrechtsgesetz einige Grundprinzipien einhalten.¹⁷ Obwohl es wahrscheinlich ist, dass diese Prinzipien im künftigen Datenrechtsgesetz nicht ausdrücklich erwähnt werden, „werden sie als Grundlage für Gesetzgebung dienen und ihren Einfluss auf das Gesetz in Bezug auf rechtliche Anpassung und rechtliche Auslegung üben“ (Hu Xuyu 2006). Das Prinzip der Legalisierung von Datenrechten spielt eine Rolle, die kein anderes Prinzip bei der Bestätigung des Eigentums und der Anpassung der Datenutzung usw. ersetzen kann und nimmt eine zentrale Position im Datenrechtssystem ein. Man kann mit Recht sagen, dass die Doktrin der Legalisierung von Datenrechten unmöglich wäre, wenn das Konzept der Datenrechte nicht existiert und ohne Doktrin der Legalisierung von Datenrechten wäre es auch unmöglich, das System

17 Unter der „Legalisierungsdoktrin“ versteht man den Legismus, den die von Gesetz festgelegten Inhalte strikt einhalten müssen. In Bezug auf Strafrecht ist der „strafrechtliche Legismus“ am wichtigsten, während im zivilrechtlichen Bereich der „sachenrechtliche Legismus“ am wichtigsten ist.

des Datenrechtsgesetzes aufzubauen. Darüber hinaus müssen wir beim Aufbau des institutionellen Systems der Datenrechte theoretische und praktische Anstrengungen kombinieren. Ein solides theoretisches System liefert die Leitphilosophie und Wertorientierung und spezifiziert die Grundprinzipien und Zielausrichtung. Ohne theoretische Führung würde das Datenrechtssystem seine Seele verlieren und desorientiert werden. Der Aufbau des Datenrechtssystems ist ein komplexes und systematisches Projekt. Es erfordert sowohl ein theoretisches System, das Leitlinien bereitstellt, als auch klare Betriebsmechanismen, die den Betriebsrahmen und den praktischen Inhalt dafür bereitstellen. Während wir das theoretische System und Betriebssystem klarstellen, sollen wir auch daran arbeiten, bestimmte Arbeitsmethoden in der Praxis des Aufbaus des Datenrechtssystems für Formulierung relevanter Regeln zusammenzufassen und ausgereifte Erfahrungen rechtzeitig zu institutionellen Vorschriften zu konzentrieren. Beim Streben nach Wert geht es hier darum, eine wirksame institutionelle Versorgung zu schaffen und die Gesetzgebung zu Datenrechten mit einer wissenschaftlichen Methodik zu unterstützen.

Der Schlüssel zur Verwirklichung von Datenrechten liegt in der Umstellung von ordnungsgemäßen Datenrechten auf gesetzliche Datenrechte und dann auf reale Datenrechte. Die Legalisierung der Datenrechte bedeutet, dass die Art und der Inhalt der Datenrechte gesetzlich vorgeschrieben werden müssen und nicht von einem anderen normativen Dokument außerhalb des Gesetzes festgelegt werden dürfen. Unter der Legalisierung der Datenrechtstypen wird verstanden, dass die Arten der Datenrechte gesetzgemäß festgesetzt werden müssen, die betreffenden Parteien dürfen keine Datenrechtsart erstellen, die von Gesetz nicht akzeptiert wird. Und sie dürfen auch nicht durch angenommene betreffende Vereinbarungen die von diesbezüglichen Gesetzen festgelegten Datenarten ändern. Das Ziel ist es, durch Gesetzgebung zu bestimmen, welche Arten von Rechten Datenrechte sind und welche nicht. In Bezug auf Legalisierung der Inhalte der Datenrechte hat sie zwei Bedeutungen: Zum einen muss der Inhalt von Datenrechten gesetzlich vorgeschrieben werden und relevante Parteien dürfen Datenrechte nicht anderweitig durch Vereinbarungen festlegen, die mit dem Inhalt der gesetzlichen Datenrechte nicht übereinstimmen.

Zum anderen dürfen die betreffenden Parteien keine Bestimmungen treffen, die den zwingenden Bestimmungen zum Inhalt der Legalisierung von Datenrechten nicht entsprechen (Long Rongyuan & Yang Guanhua 2018). Während wir außerdem verbindliche Anforderungen und direkte Bestimmungen in Bezug auf Art, Inhalt, Erwerbungsweise und andere Aspekte von Datenrechten festlegen, sollen wir bei der Gestaltung des Datenrechtssystemaufbaus auch einige grundlegende Werte und Ideen berücksichtigen.

Trennung zwischen Eigentum- und Nutzungsrecht. Mit dem digitalen, vernetzten und intelligenten Zeitalter steht unser Eigentumssystem¹⁸ vor beispiellosen Herausforderungen. In der industriellen Wirtschaft verschmelzen das Verfügungsrecht und Nutzungsrecht im Rahmen des Eigentumsrechts (Jiang Qiping 2012). Wie Mathew Ingram einmal schrieb, hatte die Digitalisierung von Musik und Video der Menschheit viel Bequemlichkeit gebracht, und jetzt hat Amazon mit seiner „Leihbibliothek“ diesen Trend in die Buchbranche gebracht. Dies ist jedoch möglicherweise nicht immer eine gute Sache. Erstens würden physische Medien allmählich

18 Die Antwort auf die Bedeutung des Eigentumsrechts findet sich in einer historischen Anspielung aus dem „Buch Lord Shang“. Es ist eine Geschichte, die Shang Yang dem König von Qin erzählte und die lautet: „Ein Kaninchen lief und Hunderte Menschen jagten hinterher. Es war nicht, weil das Kaninchen in Hunderte geteilt werden konnte, sondern weil sein Besitz nicht bestimmt wurde. Es gab viele Kaninchen auf dem Markt, aber kein Dieb wagte, es wegzunehmen. Das lag daran, dass der Besitz der Kaninchen bestimmt wurde.“ In dieser Geschichte ließ Shang Yang den König von Qin darüber nachdenken, warum ein Kaninchen im Berg von Hundert Menschen verfolgt wurde, während niemand es wagte, das Kaninchen im Käfig auf dem Markt zu berühren. Die Antwort liegt im Eigentum. Der Grund für Hundert Menschen, dem Kaninchen in den Bergen nachzujagen, war, dass sein Besitz nicht eindeutig war; aber für das Kaninchen im Käfig war sein Besitz definitiv und jeder, der das Kaninchen eines anderen nach eigenem Ermessen nahm, würde als unerlaubte Handlung angesehen. Diese Anspielung veranschaulicht die Grundfunktion des Eigentumsrechts bei der Bestimmung der sozialen Ordnung. Im Allgemeinen ist die durch das Eigentumsrecht garantierte soziale Ordnung des Eigentumsrechts die Grundlage der sozialen Ordnung, und die Regierungsführung eines Landes sollte auch mit der Schaffung eines endgültigen Eigentumsrechts beginnen. Siehe Sun Xianzhong: „Sechs Fragen in der Untersuchung des Eigentumsrechts in der Privatwirtschaft“, „Rechtswissenschaft in Finanz und Wirtschaft“, 2019, 5. Ausgabe

verschwinden; zweitens wurden die Beziehungen zwischen Benutzern und den gekauften Inhalten geändert. Was wir gekauft haben, wäre nicht das Eigentumsrecht an den Inhalten, sondern das kurzfristige Nutzungsrecht. Was hier hervorgehoben wird, ist ein wichtiges Phänomen: Im digitalen Zeitalter trennt sich das Eigentumsrecht (eigentlich das Verfügungsrecht, das Teil des Eigentumsrechts ist) vom Nutzungsrecht.¹⁹ Gegenwärtig kann eine solche Trennung in der Praxis weitgehend gefunden werden. Obwohl immer noch daran gearbeitet wird, die richtige rechtliche Struktur des Dateneigentums herauszufinden, hat die Realität bewiesen, dass das Dateneigentumsrecht nicht wichtig ist, im Gegensatz dazu, wer das Recht hat, Daten zu verwenden und welcher Wert geschaffen werden kann. „Die globale Wirtschaft neigt sich von der materiellen Welt weg und nähert sich hin zur immateriellen Bit-Welt. Es bewegt sich zugleich auch weg vom Eigentumsrecht und nähert sich zum Nutzungsrecht. Es neigt sich auch vom Wert der Kopien weg und zum Wert der Netzwerke. Und dann strömt es zu einer Welt, die unvermeidlich kommen wird, wo immer zunehmende Neuermischungen stets auftreten“ (Kevin Kelly 2016, S. 242).

Das Dateneigentumsrecht ist ein Eigendatenrecht. Es ist eine Art vollständiger und zureichender Datenrechte, während alle anderen Datenrechte unvollständig und unzureichend sind, da sie das Ergebnis der Trennung einiger Befugnisse und Funktionen des Dateneigentumsrechts sind. Die Wertorientierung der Datenrechte macht es möglich, dass die Verfügung über Daten von Datensubjekten in Wertverfügung umwandelt und ermöglicht es den Menschen, Daten auf mehrere Weise und mit höherer Effizienz zu nutzen. Die Unterteilung der Zugehörigkeit des Dateneigentums

19 Bereits im Jahr 2000 schrieb Jeremy Rifkin in „The Age of Access“: „Der bloße Gedanke, Märkte und Eigentum hinter sich zu lassen – eine konzeptionelle Änderung in der Strukturierung menschlicher Beziehungen weg vom Konzept des Eigentumsrechts hin zum Teilhabekonzept voranzutreiben – ist für viele Menschen ebenso unvorstellbar, wie die Einschließung und Privatisierung von Land und Arbeit in Eigentumsverhältnisse vor mehr als einem halben Jahrtausend gewesen war. [Allerdings] ist es wahrscheinlich, dass für eine wachsende Anzahl von Unternehmen und Verbrauchern die Idee des Eigentums in 25 Jahren begrenzt oder sogar altmodisch erscheint.“ Übersetzt von der Expertengruppe des Saidi Forschungsinstituts, CITIC Verlag, 2017, S. 241.

ist nicht der Zweck an sich, sondern ein Mittel bereitzustellen, um die Datennutzung auf institutionelle Weise zu erleichtern, um die Initiative der Datennutzer zu stimulieren, ins Spiel zu bringen und mehr Datenwert zu schaffen. Die „nutzungsorientierte Trennung“ zwischen Rechten und Funktionen wird immer häufiger. Und dieser Trend untergräbt zwangsläufig die zentrale Position des Eigentumsrechts in Datenrechtsverhältnissen. In der Zwischenzeit wird sich das Baryzentrum der Datenrechte unweigerlich vom Eigentumsrecht zu Fremddatenrechten verschieben. Es wird erwartet, dass das Datenrechtssystem vom „Besitz zur Nutzung“ und vom „Eigentumsrecht zum Nutzungsrecht“ übergeht. Die Absolutheit des Eigentumsrechts wird durch öffentliche Interessen und das öffentliche Recht des Staates immer mehr eingeschränkt. Was das relative Verhältnis zwischen dem Fremddatenrecht und dem Eigendatenrecht betrifft, so wird das erstere in gewissem Maße sicherlich Vorrang vor dem Letzteren haben. Dadurch wird der rechtliche Status der Datennutzer gestärkt, um das Recht zur Nutzung von Daten auf diejenigen zu übertragen, die die Daten effektiver nutzen können. Das Datenrechtssystem ist ein wichtiger institutioneller Faktor, der die Entwicklung der digitalen Wirtschaft fördert und einen wesentlichen Einfluss auf die Regelungen in Bezug auf Eigentum und Nutzung sowie auf die Verwirklichung des Gleichgewichts zwischen Effizienz und Fairness hat. Für das Datenrechtssystem könnte eine Überbetonung des Eigentums offensichtlich die Datennutzung verhindern und Effizienz beeinträchtigen. Eine Überbetonung der Effizienz könnte aber das Eigentum ins Wanken bringen und die Fairness gefährden. Eine Überbetonung des Eigendatenrechts würde das Fremddatenrecht bedrohend unterdrücken. Aber eine Überbetonung des Fremddatenrechts könnte das Eigendatenrecht einschränken. Daher besteht der Kern des Prinzips der Legalisierung von Datenrechten darin, das Gleichgewicht zwischen Eigentum und Nutzung, Effizienz und Fairness sowie den Eigendatenrechten und Fremddatenrechten zu halten und dadurch eine neue Datenordnung herbeizuführen.

Laut dem britischen Juristen Henry Maine gibt es drei Möglichkeiten, zwischen Recht und Gesellschaft zu koordinieren, nämlich „juristische Fiktion“, „Gerechtigkeit“ und „Gesetzgebung“ (Henry Maine 1995, S. 15). In der Überwindung der Legalisierungsdoktrin über das Sachenrecht gibt

es im Allgemeinen auch drei Wege der gesetzlichen Entwicklung.²⁰ Für die aufkommenden Datenrechte besteht der „beste Ansatz darin, Gesetz so schnell wie möglich zu erlassen“, um die wahren Merkmale von Datenrechten aufzudecken und die wesentlichen Anforderungen und der gesetzlichen Bestimmungen der Datenbeziehungen zu vereinheitlichen. Die Legalisierung von Datenrechten ist ein wichtiges Prinzip des Datenrechtsgesetzes. Und eine erstarrte Anwendbarkeit würde es unmöglich machen, sich an die Bedürfnisse der Entwicklung anzupassen. Da es zum Zeitpunkt der Gesetzgebung unmöglich ist, die Bedürfnisse der sozialen Entwicklung in der Zukunft zu antizipieren und damit ein integratives Datenrechtssystem zu schaffen. Eine strikte Einhaltung würde zwangsläufig dazu führen, dass das gesetzliche Datenrechtssystem seine Beziehungen zur Gesellschaft abbrechen würde. Insbesondere könnten einige neue Formen der Datennutzung, die in der Praxis auftreten, wegen der Einschränkungen der Legalisierung von Datenrechten wahrscheinlich nicht rechtzeitig zu Datenrechten gesteigert werden und die daraus resultierenden Datenrechtsstreitigkeiten könnten auch schwierig zu behandeln sein. So könnte dies zu sozialer Anomalie und Unordnung führen. Die Datenbeziehungen könnten immer komplizierter werden und das Datenrechtssystem könnte auch nicht in der Lage sein, alle Arten von Datenrechten detailliert festzulegen. Daher können wir uns bei der Anerkennung von Datenrechten nicht vollständig auf Gesetzgebung verlassen. Das heißt, wenn wir das Prinzip der Legalisierung von Datenrechten formulieren, sollen wir einerseits mit diesem Prinzip im Klaren sein und andererseits sollen wir die Durchsetzbarkeit und Offenheit der Legalisierung von Datenrechten berücksichtigen,

20 Legal Fiction soll die Koordination zwischen Recht und Gesellschaft hauptsächlich durch Auslegung von Rechtsvorschriften erreichen. In zivilrechtlichen Ländern manifestiert sich die Methode der Gerechtigkeit als Rolle der Leitwirkung der allgemeinen Grundsätze auf die Festlegung spezifischer Normen. Und die Anwendung dieser Grundsätze als allgemeine Bestimmungen des Zivilrechts spielt die Rolle der Überwindung der Beschränkungen von Positivgesetzen. Wenn in der sozialen Entwicklung neue Arten von Rechten entstehen, kann deren rechtzeitige Legalisierung die Starrheit des legalistischen Systems des Sachenrechts mindern. Siehe Yang Yuxi: „Über den Legalismus des Sachenrechts“, „Forschung über Vergleichsmethode“, 2002, 1. Ausgabe

damit das Prinzip noch eine gewisse Flexibilität enthalten und so an die sich stets ändernde Außenwelt anpassen kann, weil kein System geschlossen oder ultimativ ist. Und das gilt auch für das Datenrecht.

Literaturverzeichnis

- Adam Smith: „Theorie der moralischen Gefühle“, Übersetzt von Jiang Ziqiang et al. Die kommerzielle Presse, 2015.
- Adam Smith: „Untersuchung über die Natur und Ursachen des Reichtums der Nationen“, (Band I), übersetzt von Guo Dali u. Wang Yanan, Die kommerzielle Presse, 1997.
- B. Schwartz: „Geschichte des amerikanischen Rechts“, übersetzt von Su Yanxin. Verlag der chinesischen Universität für Politikwissenschaft und Rechtskunde, 1989.
- Chen Zhonglin: „Freiheit, Menschenrecht, Rechtsstaatlichkeit: Interpretation der menschlichen Natur“, in „Moderne Rechtswissenschaft“, 3/2001.
- Cheng Enfu: „Analyse der westlichen Theorie der Eigentumsrechte“, Zeitgenössisches China-Verlagshaus, 1997.
- David C. Vladeck, „Machines without Principles: Liability Rules and Artificial Intelligence“, *Washington Law Review*, 2014 (89)
- David Hume: „Theorie der menschlichen Natur“, übersetzt von Guan Wenyun, Die kommerzielle Presse, 1996.
- Francis Bacon: „Textsammlung von Bacons Essays“, übersetzt von Shui Tiantong, Die kommerzielle Presse, 1983.
- Gao Chengjun: „Unterschiede zwischen chinesischen und westlichen Rechtskulturen aus Perspektive der Hypothese der menschlichen Natur“, in *Journal des Institut für Politikwissenschaft und Recht Gansu*, 4/2014.
- Guo Jing: „Der menschliche Wert des gegenseitigen Altruismus“, in *Nachrichtenübermittlung zu Dialektik der Natur*, 11/2005.
- Gustav Radbruch: „Bonmotssammlung der gesetzlichen Weisheit“, übersetzt von Shu Guoying, Verlag des chinesischen Rechtssystems, 2001.
- Han Dongping: „Das Geheimnis des Menschen lösen: Dekonstruktion und Rekonstruktion der Definition des Menschen“, in *Wuhan University Journal (Humanity Sciences)*, 6/2016.
- Henry Maine: „The antike Law“, übersetzt von Shen Jingyi, Shangwu Buchhaus, 1995.

- He Xiaorong u. Chen Quansheng: „Forschung und Analyse von Umweltgesetz im Blickwinkel des ‚Ökomenschen‘“, in „Journal der Fuzhou Universität“, Philosophie und Sozialwissenschaft, 1/2009.
- Holmes Rolston: „Umweltethik“, übersetzt von Yang Tongjin, Der Chinesische Sozialwissenschaftliche Verlag, 2000.
- Hoshino Echi: „Mensch im privaten Recht – mit Eigentumsrecht des Zivilgesetzes als Zentrum“, übersetzt von Wang Chuang, Verlag der chinesischen Rechtssysteme, 2004, S. 21.
- Hu Xuyu: „Wertentwicklung und Analyse von Rationalität der Legalisierung der Rechte der Dinge“, in „Forum der Rechtskunde“, 2/2006.
- Hu Yuhong: „Einführung in die Methodik der Rechtswissenschaft“, Volksverlag Shandong, 2002.
- Hu Yuhong: „Erklärung der Rechtsphilosophie der „Individuen“. Volksverlag Shandong, 2008.
- Huang Tao: „Von der Hypothese der Wirtschaftsperson zur Hypothese der Koop-Person“, in Reform des Wirtschaftssystems, 2/2009.
- Immanuel Kant: „Religion innerhalb der Grenze der reinen Vernunft“, übersetzt von Li Qiuling, Verlag der chinesischen Renmin Universität, 2003.
- Jeremy Rifkin: „Die Null-Grenzkosten-Gesellschaft“, übersetzt von der Expertengruppe des Chinesischen Zentrums für Entwicklung der Informationsindustrie, CITIC Verlag, 2017.
- Jiang Qiping: „Dateneigentum erfordert Trennung des Herrschaftsrechts vom Nutzungsrecht“, in China Internet-Wochenzeitschrift, 5/2012.
- John Jordan: „Machine-man and Human“, übersetzt von Liu Yuchi, Verlag der chinesischen Renmin Universität, 2018.
- Kevin Kelly: „Unvermeidlich“, übersetzt von Zhou Feng et al. Elektron-Industrie Verlag, 2016.
- Karl Marx: „Manuskripte der Ökonomie und Philosophie 1844“, in „Gesammelte Werke von Marx und Engels“ Band 46 vom zentralen Kompilation- und Übersetzungsbüro, Volksverlag 1979.
- Laura E. Quarantiello: „Cyberkriminalität: Wie Sie sich vor Computerkriminalität schützen können“, übersetzt von Wang Yong, Erziehungsverlag Jiangxi, 1999.
- Li Guojie: „Datenteilhabe: Voraussetzung für die Modernisierung des staatlichen Verwaltungssystems im Big-Data-Zeitalter“, in China Information Wochenschau, 25. August 2014.
- Long Rongyuan u. Yang Guanhua: „Studie über Datenrechte, Datenrechtssystem und Datenrechtsgesetz“, Journal of Law and Technology, 5/2018.
- Ludwig Andreas Feuerbach: Eine Auswahl von Feuerbachs philosophischen Werken (Bd. 1). übersetzt von Rong Zhenhua et al. Die kommerzielle Presse. 1984.

- Ma Changshan: „Die vierte Generation der Menschenrechte und ihre Garantie vor dem Hintergrund einer intelligenten Gesellschaft.“ *China Legal Science*, 5/2019.
- Phil McNally, Sohail Inayatullah, „The Rights of Robots“, *Futures*, 1988 (20).
- Qiu Zeqi: „Auf dem Weg zur digitalisierten Gesellschaft. Im Forum der Informationsgesellschaft 50: Die Zukunft ist gekommen: Wiederaufbau und Innovation im Zeitalter von „Internet Plus“. Shanghai Fernosten Publishers, 2016.
- Ray Kurzweil: „Die Singularität ist nahe: Wenn Menschen die Biologie überschreiten“, Übersetzt von Li Qingcheng et al. China Machine Press, 2015.
- Ray Kurzweil: „Wie man einen Geist erschafft“, übersetzt von Sheng Yangyan, Volksverlag Zhejiang, 2014.
- Robert Morrison MacIver: „Politologie“, übersetzt von Chen Qitian, China Buchhaus, 1946.
- Shen Zhai: „Von der ‚Person der Ethik‘ zur ‚Person der Wissenschaft‘: Über den Wandel des Menschen im neuzeitlich-modernen chinesischen Recht am Beispiel des Zivilrechts“, in *Pazifik Journal*, 8/2011.
- Sun Weiping: „Reflektion zum Wert der künstlicher Intelligenz“, „Philosophische Forschung“, 10/2017.
- Sun Xianzhong: „Sechs Fragen in der Untersuchung des Eigentumsrechts in der Privatwirtschaft“, „Rechtswissenschaft in Finanz und Wirtschaft“, 5/2019.
- Thomas Nagel: „The Possibility of Altruism“, Princeton University Press, 1978.
- Wang Dingding: „Vorlesungen über Grundlage der institutionellen Analyse“, Volksverlag Shanghai von Shanghai Century Publishing (Group) Co., Ltd. 2005.
- Wang Liming: „Neue Herausforderung für das Zivilrecht im Zeitalter der künstlichen Intelligenz“, in *Orientalisches Recht*, 3/2018.
- Wang Tianen: „Informationszivilisation: Ein Schlüssel zu einem neuen Verständnis von Entwicklung“, in *Sozialwissenschaften in China*, 6/2018.
- Wu Xianjing: „Theoretische Implikationen der Ökoperson und ihre Bedeutung für das Umweltgesetz“, in *Law Review*, 4/2010.
- Xia Xiaoxiong: „Modernisierung des Gesellschaftsrechts: Institutionelle Reform, Systemrekonstruktion und Umgestaltung des Geistes“, *Northern Legal Science*, 4/2019.
- Xie Hongfei: „Der ‚Mensch‘ im modernen Zivilrecht“, in *Peking University Law Review*, 2/2002.
- Xie Zaiquan: „Über die zivilrechtlichen Eigentumsrechte“, Verlag der chinesischen Universität für Politikwissenschaft und Rechtswissenschaft, 1999.
- Yan Chunsheng: „Rechtsgrundlage aus Sicht der menschlichen Natur“, Verlag des chinesischen Rechtssystems, 2016.

- Yang Chunxue: „Wiedergeburt‘ des Wirtschaftsmenschen: Untersuchung und Verteidigung für eine neue Zusammenfassung“, in „Wirtschaftsforschung“, 11/2005.
- Yan Cunsheng: „Moralität: Menschlichkeitsdimension des Rechts – über das Verhältnis von Recht und Moral“, in Rechtswissenschaft – Journal der Nordwesten Universität der Politikwissenschaft und Rechtskunde, 1/2007.
- Yan Cunsheng: „Moralität: Menschlichkeitsdimension des Rechts – über das Verhältnis von Recht und Moral“, in Rechtswissenschaft – Journal der Nordwesten Universität der Politikwissenschaft und Rechtskunde, 1/2007.
- Yang Lan: „Wie Marx die Natur des Menschen definierte“, in Volksforum, 8/2018.
- Yang, Yuxi: „Über Legalisierung des Sachenrechts“, in „Zeitschrift für Rechtsvergleichende Studie“, 1/2002.
- Yi Jun: „Individualistische Methodik und Privatrecht“, in „Forschung über Rechtswissenschaft“, 1/2006.
- Yu Chengfeng: „Vom Prozess gegen eine Ratte zum Gesetz über künstliche Intelligenz“, in Buchlesen, 7/2017.
- Yu Zhong: „Veränderung und Vergleich: im Text der Verfassung dargestellte Person“, in Studie über Rechtswissenschaften und Wirtschaftswissenschaften, 5/2009.
- Yuval Noah Harari: „Homo Deus: Eine kurze Geschichte von morgen“, übersetzt von Lin Junhong, CITIC Verlag, 2017.
- Zentrales Büro für Zusammenstellung und Übersetzung Gesammelte Werke Marx & Engels (Bd. 1). Volksverlag, 2009.
- Zentrales Büro für Zusammenstellung und Übersetzung Sämtliche Werke von Marx und Engels (Bd. 23). Volksverlag, 1972.
- Zhang Jianwen: „Beitrag und Grenze des Grishen Gesetzantrags – Kommentar zum Entwurf des ersten Robotergesetzes Russland“, in Journal der Huadong Universität der Politikwissenschaft und Rechtskunde, 2/2018.
- Zhang Yujie: „Über Rechtsordnung für Rechte und Risiken von Robotern im Zeitalter der künstlichen Intelligenz“, in Orientalisches Recht, 6/2017.
- Zhou Xiang: „Intelligente Roboter als Rechteinhaber“, In Rechtswissenschaft, 10/2019.
- Zhu Xiaozhe: „Der Mensch im Sozialgesetz - zugleich über Veränderung der modernen Gesellschaft und gesetzlichen Persönlichkeit“, in „Rechtswissenschaft“, 8/2002.
- Zhuo Zeyuan: „Einleitender Überblick über den Wert des Gesetzes“, Volksverlag, 2001.

Datenrecht

Der Fortschritt der Wissenschaft und Technologie zwingt die Menschen ständig dazu, den Umfang der Rechte zu erkunden. Mit der Vertiefung der Untersuchung sind sich die Menschen nicht nur ihrer Rechte bewusster, sondern sich der traditionelle Umfang der Rechte auch ändert. Insbesondere eine neue Sache tritt in den Bereich der Rechtsbeziehungen ein, die sich sowohl von physischen Dingen unterscheidet, als auch Menschen übertrifft. Das sind „Daten“. Daten können nicht nur als Subjekt der gesetzlichen Regelung gelten, sondern auch zu einer neuen Form von Rechten führen. Die derzeitige Frage ist, welches Metakonzept für die gesetzliche Bestätigung der Rechte an Daten zu wählen ist. „Mit der Aufstellung der Datenrechte entfernen wir die Datenrechte von der Positionierung der Dateneigentumsrechte, die die traditionellen Theorien über Persönlichkeitsrechte und Eigentumsrechte etc. als ihren logischen Ausgangspunkt genommen hat. Im ganzen System der Rechte haben Datenrechte unabhängige Stellung und umfassen Datenrechte, Teilhaberechte und Datenhoheit“. Datenrechte haben die Merkmale privater Rechte, öffentlicher Rechte und Souveränität, die sich jeweils als „Datenrechte“, „Datenmacht“ und „Datensouveränität“ manifestieren. Die Datenrechte und Datenmacht stehen oft in gegenseitiger Konfrontation, im Wettbewerb und suchen ständig nach einem Gleichgewicht. Je nach ihren Arten können die Datenrechte normalerweise in persönliche Datenrechte, Unternehmensdatenrechte und Regierungsdatenrechte unterteilt werden. Deshalb ist es sehr wichtig, verschiedene Datentypen klar zu definieren, Möglichkeiten zur Schaffung einer angemessenen Struktur für Datenrechte zu untersuchen und ein entsprechendes Rechtssystem für den Datenschutz zu analysieren, um nach einem Gleichgewicht dazwischen zu suchen.

Abschnitt I Datenrecht und Datenmacht

Das Recht gehört zur gesetzlichen Kategorie, während die Macht ein politischer Begriff ist. Indem wir die Normalform „Recht-Macht“ einführen, erleichtern wir es den Menschen, einen Mindestkonsens über die Grundbegriffe zu erzielen, auf die sich bei der rechtswissenschaftlichen Untersuchung von rechtlichen Fragen in Bezug auf Daten beziehen, um mittels kompatibler Konzeptsysteme, Beobachtungsperspektiven und Forschungsmethoden usw. rechtliche Fragen in Bezug auf Datenrechte zu erklären und zu lösen (Wen Yuheng 2019). Die menschliche Gesellschaft tritt eben in eine neue Phase ein, die vor allem von Datenproduktivität geprägt ist. Die Menschen haben begonnen, die Beziehungen zwischen Menschen und Daten zu überdenken und über das Thema Datenrechte und Datenmacht nachzudenken. Daten sind sowohl eine Normalform für Recht, als auch eine Machtschilderung. Konkret gesagt sind Daten ein neuer Produktionsfaktor, eine neue Ressource für Innovationen, eine neue Organisationsform, eine neue Art von Rechten und eine neue Manifestation von Macht. Die Datennutzung ist zu einem wichtigen Weg geworden, wie Menschen ihren Wohlstand steigern können, während der Schutz von Datenrechten und die Einschränkung der Datenmacht zu einem wichtigen Merkmal der digitalen Zivilisation geworden sind.

(I) Von Zahl zu Datenrecht

1. Zahl: Der Ursprung aller Dinge

Zahl ist ein Begriff, der entstand, bevor die Menschheit versuchte, die objektive Welt zu verstehen. In menschlichen Produktionsaktivitäten wie Sammeln und Jagen begann der Begriff der Zahl zu keimen, indem Menschen verschiedene Arten von Dingen verglichen. „Die Menschen erkannten nach und nach, dass die Dinge einige Gemeinsamkeiten aufweisen, d.h. die Einheit der Dinge, wobei sie auch erkannten, dass Dinge unterschiedlicher Art auch quantitativ etwas gemeinsam haben, beispielsweise

die entsprechende Beziehung, die sich quantitativ zwischen ihnen bilden kann. Diese abstrakte Natur der Quantität, die die Dinge verschiedener Art gemeinsam haben, ist Zahl“ (Liu Hong & Hu Xinhe 2013). Der britische Philosoph Bertrand Russell verallgemeinerte diese abstrakte Natur mit den Worten: „Nur in einem hohen Stadium der Zivilisation können wir diese Reihe (natürliche Zahlenreihe) als Ausgangspunkt unserer Entdeckung nehmen“ (Bertrand Russell 1982, S. 8). Bereits im alten Ägypten, Rom und China begannen die Menschen mit der Verwendung der Zahlen, um die Regeln und Beziehungen in der Welt zu interpretieren, und begannen allmählich, Zahlen für Aktivität wie Handel, Zählung und Statistik etc. zu verwenden.

„Das Konzept der Zahl im menschlichen Gehirn ist der erste Versuch der Menschheit, den Ursprung der Welt zu verfolgen und darüber nachzudenken“ (Gao Jianping & Qi Zhiyuan 2019). Dies ist der philosophische Ursprung des Sprichworts der pythagoreischen Schule, dass „alles Zahl ist“. Pythagoras hat die Zahl in ontologischer Hinsicht zur Position des Ursprungs aller Dinge erhoben, wobei die Zahl nicht als qualitative Regel betrachtet wurde, sondern als ein Attribut, das in alle Dinge durchdringt und die gemeinsame Eigenschaft der Dinge darstellt. Die Substanz der Dinge könnte verschwinden, aber die Zahl hat keinen Anfang und kein Ende. Sie kann verwendet werden, um alles zu interpretieren, alles zu tragen und alles zu kontrollieren. Dass unter „alles ist Zahl“ verstandene Zahl nicht nur als normale Berechnungsmethode, sondern auch als Weg, der die Menschheit dazu bringt, alle Dinge auf Grundlage der Zahl zu verstehen. Sie haben die gemeinsame Eigenschaft aller Dinge gefunden, nämlich die Zahl. Die Zahl ermöglichte das menschliche Gehirn, alles zu verallgemeinern, die Welt zu verstehen, die Welt proportional zu planen und sie harmonisch wie Zahl aufzubauen. Nach Ansicht von Pythagoras ist die Zahl nicht nur der Ursprung der realen Welt, sondern auch die Quelle der virtuellen Welt, die durch moderne Wissenschaft und Technologie geschaffen wurde. Oder anders gesagt, sie ist der Ursprung der menschlichen spirituellen Welt. Mit anderen Worten, die Zahl ist der Ursprung aller Dinge auf der Welt.

Im Prozess des digitalen Aufbaus einer virtuellen Welt scheint jeder Schritt die Idee widerzuspiegeln, dass „alles Zahl ist“. Die Anzahl durchläuft

jede Phase des gesamten Prozesses, von der grundlegenden Zählungsmethode über die Berechnung bis hin zur Modellierung sowie bis zur dargestellten Methode und letztendlich zur Speicherung und Kommunikation. Und „alle betroffenen Dinge haben ihre eigenen Zahleninformationen“. „Alles andere zeigt, dass sie in der gesamten Natur eine Nachahmung von Zahlen sind“ (Ru Xin 2005, S. 39). Elemente in der virtuellen Welt werden in Form digitaler Informationen gespeichert, dadurch erleichtert wird, diese später in digitaler Form gelesen werden können. Dies scheint die Kenntnisse von Pythagoras, „Zahl ist der Ursprung aller Dinge“, auf dem Computer mechanisch zu demonstrieren und verwirklicht auch das Ideal, dass Zahl in der modernen digitalen Welt als Regel dient.

2. Von Daten zu Big Data

Daten repräsentieren das Verständnis des Menschen für die Kausalzusammenhänge in der objektiven Welt. Daten sind in gewissem Sinne die Erstreckung und Erweiterung des Zahlenbegriffs und ein zwangsläufiges Produkt der Entwicklung der menschlichen Sozialwissenschaft, wenn sie ein bestimmtes Stadium erreicht. „Die Strömung der Informationstechnologie mit der Mikroelektronik, elektronische Kommunikation und Computertechnologie etc. als Zentrum hat zu einer neuen Runde der technologischen Revolution geführt und die Menschheit allmählich in die Informationsgesellschaft gedrängt“ (Zhang Xinbao 2015). Zu diesem Zeitpunkt entstand die moderne Denkweise, die sich auf Daten konzentrierte, und „Ausdruck mit Daten“ wurden zum Kern der Methodik, mit der Menschen die Welt erkennen. Das Wort „Daten“ kommt vom lateinischen Wort „datum“, das erstmals im 13. Jahrhundert vorkam und etwas Gegebenes bedeutete. Aus philosophischer Sicht sind „Daten das Produkt menschlicher kognitiver Aktivitäten, eine subjektive Reflexion objektiver Dinge und eine logische Sprache zur Darstellung von Dingen und Phänomenen“ (Liu Hong & Hu Xinhe 2013). Auf dem Gebiet des Computers beziehen sich Daten im Allgemeinen auf jedes Material, das vom Computer verarbeitet werden kann, einschließlich aller Arten von Wörtern, Zahlen, Diagrammen usw. Es ist ersichtlich, dass Daten aus den Erfordernissen stammen, die die objektive Welt aufzeichnen.

Daten werden in der menschlichen Praxis als Werkzeug verwendet. Sie durchbrechen die symbolisch spezifische Eigenschaft, gehen über Zeit und Raum hinaus und werden zur Grundlage der Ableitung von Regeln für die Bewegung und Veränderung von Dingen, um letztendlich unsere moderne Gesellschaft und Zivilisation zu etablieren.

Big Data enthält das kognitive Verständnis der Menschheit für die Gesamtheit der Beziehungen in der objektiven Welt. „Big Data ist eine Sammlung von Daten, die vor allem durch große Mengen, mehrere Typen, schnellen Zugriff und einen hohen Anwendungswert gekennzeichnet sind. Es entwickelt sich schnell zu einer Art Informationstechnologie der neuen Generation und zu einem Modell der Dienstleistungsindustrie, das die Erfassung, Speicherung und Zusammenhangsanalyse von massiven Daten aus verstreuten Quellen und in verschiedenen Formaten abdeckt, wobei das Ziel ist, neues Wissen zu entdecken, neuen Wert zu schaffen und neue Fähigkeiten hervorzubringen“ (Staatsrat der Volksrepublik China 2015). Big Data ist eine neue Stufe der Informationsentwicklung. Sie ist jetzt kein neues Konzept mehr, sondern läutet eine neue Ära ein, stellt eine mehrdimensionale unendliche Variable dar und fördert die Menschheit, den Fokus bei ihrer Erkenntnis der objektiven Welt von kausalen Beziehungen auf Korrelationen zu verlagern und auf der „Basis der systematischen Methode und gestützt auf der ‚Beziehung‘ von Teil mit Teil, Teil mit dem Ganzen und System mit Umgebung die objektive Welt zu untersuchen. Daten als Werkzeug, mit dem Menschen die Welt erkennen, beschreiben objektive Dinge, die nur den subjektiven Teil der Welt ausmachen, nicht aber die gesamte Welt. Im Gegenteil hilft Big Data den Menschen, den Umfang ihrer Erkenntnis in Zeit und Raum zu erweitern und ihr Wissen über die Welt von Teilen auf das Ganze zu erstrecken“ (Gao Jianping & Qi Zhiyuan 2019).

Auf der vierten Plenartagung des 19. Zentralkomitees der KP Chinas wurde darauf hingewiesen, dass „es notwendig ist, den Mechanismus zu verbessern, bei dem die Beiträge von Produktionsfaktoren wie Arbeit, Kapital, Land, Wissen, Technologie, Management und Daten vom Markt bewertet und die Vergütung nach Beiträgen festgelegt werden sollen“. Das ist das erste Mal, dass das CPC-Zentralkomitee Daten als Produktionsfaktor anerkennt, die zum Beitrag zählen und damit für Einkommensverteilung gelten können. Einerseits können Daten als eine Art Ressource das

globale Wirtschaftswachstum und die soziale Entwicklung in verschiedenen Ländern fördern, genau wie Land, Arbeit, Kapital und andere Produktionsfaktoren. Andererseits bilden Daten als konstruktive Kraft für soziale Beziehungen den Kern unserer Zeit und gelten zusammen mit Material und Energie als drei wesentliche Elemente menschlicher Aktivitäten in der natürlichen Welt. So werden Daten von einer Art Symbol, das Dinge beschreibt, in etwas Wesentliches für alle Dinge auf der Welt umgewandelt. Big Data ist eine Sammlung von Daten und mehr als Daten. Big Data ist zu einer wichtigen Kraft geworden, die unsere heutige soziale Ordnung wieder aufbaut und die Menschheit in die Ära der digitalen Zivilisation führt. Big Data mit ihrer inklusiven Eigenschaft wird die bestehenden Grenzen zwischen Ländern, Regierungen, Organisationen und der Öffentlichkeit sprengen. Der größte Effekt, den Big Data ausübt, ist, dass sie ‚eine gemeinsame Welt‘ für uns alle geschaffen hat, eine Welt, die wir auf jeden Fall nur gemeinsam nutzen können“ (Beck, Deng Zhenglai & Shen Guolin 2010). Im Zeitalter von Big Data hat sich der Schwerpunkt der Wettbewerbe zwischen Ländern von Kapital, Land, Bevölkerung und Ressourcen auf Daten verlagert. Basierend auf ihren Datenfähigkeiten werden Länder in Gruppen von „datenmächtigen Ländern“ und „datenschwachen Ländern“ eingeteilt. Die globale Landschaft wird sich dramatisch verändern.

3. Die Einleitung der Datenrechte

Da Daten ständig zu einer Art von Ressource, Vermögenswert und Kapital werden, ist eine Verlagerung von Daten zu Datenrechten zu einem unvermeidlichen Trend geworden, als sich die Menschheit in Richtung der digitalen Zivilisation bewegt. Es ist auch der allgemeine Trend, dass Daten zu Rechten, zu Macht und zur Institutionalisierung werden. Die Datenordnung wird zur obersten Ordnung in der zukünftigen Gesellschaft. Es gibt vier „neue Dinge“ bei Datenrechten: Erstens stellen Datenrechte ein neues Rechtsobjekt dar; zweitens sind Datenrechte eine neue Art von Rechten; drittens stellen Datenrechte neue Arten von Rechtsattribut dar; und viertens enthalten Datenrechte neue Art von Funktion und Kompetenz (siehe Tabelle 2-1). Datenrechte sind die Vorbedingung für Festlegung von Datenregeln und ein wichtiger Eckpfeiler, um „die Entwicklungsmöglichkeiten der Digitalisierung, Vernetzung und intelligenten Entwicklung zu

Tabelle 2-1 Wahrzeichen von Datenrechten

Wahrzeichen	Grundzüge
Objekt des Rechts	<p>Daten sind kein „Ding“ im Sinne des Zivilrechts (d. h. kein Objekt des Sachenrechts). Sie sind weder ein physisches Objekt in der Physik noch ein immaterielles Objekt, wie es in den geistigen Eigentumsrechten beschrieben ist. Daten sind eine unabhängige objektive Existenz und bilden eine digitale Welt, die jenseits der physischen und spirituellen Welt liegt. Das Subjekt des Datenrechts ist bestimmter Rechtsinhaber, einschließlich der spezifischen Objekte, um die es in Daten geht, und derjenigen, die die Daten sammeln, speichern, übertragen und verarbeiten usw. (einschließlich natürlicher Personen, juristischer Personen und nichtjuristischer Körperschaften). Unterschiedliche Datensubjekte verfügen über unterschiedliche Befugnisse. Die Objekte von Datenrechten sind bestimmte Datensätze. Daten sind eine Kombination aus einer Reihe von Ziffern, Codes, Bildern und Texten etc. Einzelne Ziffern oder Codes haben keinen Wert, und der Wert kann nur mit der Neuvermischung durch Kombinieren, Integrieren und Zusammensetzen erzeugt werden. Daher sollten die Objekte von Datenrechten bestimmte Datensätze mit Regeln und Wert sein.</p>
Art des Rechts	<p>Nach der gesetzlichen Auslegung im traditionellen Sinne können Menschenrechte in zwei Typen eingeteilt werden: Persönlichkeitsrecht und Eigentumsrecht. Im digitalen Zeitalter hinterlässt die Menschheit in unterschiedlichem Maße „digitale Fußspur“ in verschiedenen Arten digitaler Ökosysteme. Einerseits sind diese Daten Fragmente menschlichen Verhaltens, wichtige Aufzeichnungen über persönliche Teilnahme an sozialen Aktivitäten und ein wichtiger Weg für Erstreckung der Persönlichkeit. Daher ist es notwendig, Datensubjekte als menschliche Würde zu wahren und sicherzustellen, dass sie das Recht darauf hat, ihre Freiheit nicht gelehrt, ihr Ruhm nicht beleidigt, ihre Privatsphäre nicht ausspioniert und ihre Information nicht missbraucht zu werden. Andererseits sind Daten auch wichtige soziale Ressourcen. „Daten haben Wert“ und können den Dateneignern wirtschaftliche Vorteile bringen. Daher müssen Rechte auf Dateneigentum gewährt werden. Damit gelten Datenrechte als umfassende Rechte, die sowohl Persönlichkeitsrechte als auch Vermögensrechte zusammen integrieren.</p>

(Fortsetzung)

Tabelle 2-1 Fortsetzung

Wahrzeichen	Grundzüge
Attribut des Rechts	Datenrechte sind eine Kombination aus öffentlicher Macht und privaten Rechten. Dazu gehören sowohl die Datenhoheit, die die nationale Würde widerspiegelt, als auch das Recht auf Daten, die das persönliche Wohl hervorheben. Daher sollte die gesetzliche Eigenschaft der Datenrechte nicht nur als eine Art privatrechtlich geregelte Persönlichkeitsrechte, sondern auch auf der Ebene des Gesichtspunkts der vom öffentlichen Gesetz geregelten staatlichen Sicherheit analysiert werden. Das heißt, Datenrechte erfordern sowohl eine privatrechtliche Selbstregulierung als auch die Einmischung von öffentlichem Recht.
Funktion des Rechts	Dingliche Rechte besitzen die Exklusivität wie Monopol, daher kann es niemals zwei Eigentumsrechte an einem Objekt geben. Jeder ist verpflichtet, das absolute Verfügungsrecht der Rechteinhaber auf Objekte nicht zu beeinträchtigen. Datenrechte sind aber nicht mehr ein Monopolrecht. Sie sind teilhabbare Rechte, die nicht exklusiv sind. Dies äußert sich in den „Mehrrechten auf die gleichen Daten“, die den Kern und das Wesen der Datenrechte bilden. Das Vorbringen dieser wichtigen rechtstheoretischen These „Datenrechte sind im Wesentlichen Teilhaberechte“ wird ein symbolisches historisches Ereignis sein, mit dem die Regeln der menschlichen Zivilisation umgeschrieben werden.

Quelle: von den Autoren

nutzen und die Herausforderungen der Big-Data-Entwicklung in Bezug auf Gesetz, Sicherheit und Regierungsverwaltung zu bewältigen“.

Es sollte besonders darauf hingewiesen werden, dass Datenrechte das Attribut privater Rechte, öffentlicher Rechte und Souveränität aufweisen. Im Bereich der privatrechtlichen Eigenschaft werden Datenrechte in personenbezogene Datenrechte und Unternehmensdatenrechte unterteilt, je nachdem, wer die Daten besitzt, während die persönlichen Datenressourcen und Unternehmensdatenressourcen als Objekte dieser Datenrechte betrachtet werden. Im Bereich der öffentlichen Rechte weisen Datenrechte klare öffentliche und kollektive Merkmale auf. Der Staat und die Regierung gelten als Ausführungssubjekt und mit der Maximierung der öffentlichen Interessen als Wertorientierung. Sie gelten als eine kollektive Macht, die die Ordnung für Teilnahme an öffentlichen Angelegenheiten energetisch

aufrechtzuerhalten und durch Selbsterweiterung gekennzeichnet zu sein. Die souveräne Eigenschaft der Datenrechte manifestiert sich darin, dass die Datensouveränität ein wichtiger Bestandteil der staatlichen Souveränität ist. Als eine notwendige Ergänzung der staatlichen Souveränität bereichert und erweitert Datensouveränität die Konnotation und Epitaxie der traditionellen staatlichen Souveränität. Sie ist eine unweigerliche Wahl, damit die Staats-souveränität der modernen virtuellen Cyberspace-Verwaltung anpassen und die Unabhängigkeit der staatlichen Souveränität gewahrt werden kann.

„Ob ein neues Recht oder eine neue Macht geschaffen werden kann, hängt letztendlich davon ab, ob die Produktionsaktivität zu einer Steigerung des materiellen Wohlstands führen kann, wodurch neue Interesseneinheiten entstehen und Zinsforderungen realisiert werden können“ (Dong Zhiwei 2001, S. 297). Auf Grundlage des „Datenmenschen“ können entsprechende Rechte und rechtliche Beziehungen mit der Datenermächtigung entstehen, wie zum Beispiel Datenrechte, Teilhaberechte und Datenhoheit usw. Die Datenrechte hier sind kein unabhängiges System von Rechten, sondern eine Art beabsichtigte Rechte auf der Grundlage, die das auf der Basis des Datenraums entstandene aktuelle Gesetzsystem nicht regeln kann. Die Streitigkeiten über Datenrechte, die nach dem Abbruch dieser Absichtsrechte vom bestehenden Rechtsschutzsystem entstehen, könnten aufgrund fehlender rechtlicher Maßnahmen, die mit neuen Datenverarbeitungsverhalten vereinbar sind, zu einer Art von neuen Streitigkeiten führen. Als neue Rechtsbeziehungen entstehen, werden die traditionellen Rechtsbeziehungen unüberwindlichen Systemhindernissen gegenüberstehen und nicht in der Lage sein, mit den neuen Beziehungen umzugehen. Daher ist es notwendig, ein praktisches und wirksames System für Steuerung und Regulierung von Daten aufzubauen.

(II) Rechte an Daten

1. Datenrechte sind eine neue Art von Rechten

Die Rechte auf Daten entstehen mit der Entstehung von Daten und werden mit der Entwicklung von Big Data hervorgehoben. Die Rechte auf Daten sind sowohl verfassungsmäßige Rechte als auch bürgerrechtliche Rechte. Sie sind eine neue Art von Rechten, die sowohl Persönlichkeitsrechte als

auch Eigentumsrechte enthalten. Zu Inhabern der Datenrechte gehören die von Daten bestimmten spezifischen Objekte, sowie diejenigen, die die Daten sammeln, speichern, übertragen und verarbeiten etc. Unterschiedliche Rechtssubjekte haben unterschiedliche Befugnisse. Objekte der Datenrechte sind bestimmte regelmäßige und wertvolle Datensätze, damit sind meistens personenbezogene Daten gemeint. Die Kernrechte, die von ihnen geschützt werden, sind Rechte auf personenbezogene Daten. Die persönlichen Datenrechte sind in Ländern des kontinental-europäischen Rechtssystems allgemein anerkannt und werden in der Gesetzgebung als Grundrecht angesehen. Die persönlichen Datenrechte sind verfassungsmäßige Rechte. Artikel 38 der „Verfassung“ der Volksrepublik China hat die verfassungsrechtliche Grundlage dafür geboten, dass das persönliche Datenrecht zu einem Grundrecht wird.¹ Darüber hinaus betonen die persönlichen Datenrechte die Unabhängigkeit der Persönlichkeit und der Verhaltensfreiheit des Einzelnen, entsprechen den persönlichen Interessen im Privatrecht und der Grundwertorientierung für Verhaltensfreiheit, diese zu genießen und zu verwirklichen. So ist das auch ein ziviles Recht. Wenn Daten als Vermögenswert betrachtet werden, sind sie einzigartig, da sie allgemeingültig, extern und nicht ausschöpfend etc. sind. Auf dieser Grundlage und im idealen Zustand des reinen akademischen Abzugs, können die vollständigen Datenrechte je nach der Art und Weise der Anwendung in mehrere Bündel von Rechten, wie zum Beispiel das Recht auf Besitz, das Recht auf Nutzung, das Recht auf Gewinn, das Recht auf Teilhabe und das Recht auf grenzüberschreitende Übertragung usw. aufgeteilt werden. Die Rechtsinhaber können ein oder mehrere Rechtsbündel gleichzeitig

1 Professor Lin Laifan ist der Meinung, dass der Inhalt von Artikel 38 der „Verfassung“ in zwei Teile aufgeteilt werden kann: der erste Teil lautet: „Die Würde der Persönlichkeit von Bürgern der Volksrepublik China ist unantastbar“, das ist ähnlich wie der Ausdruck, dass der Inhalt des grundlegenden Verfassungswerts wie die deutsche „menschliche Würde“ zum Ausdruck gebracht wird; der letztere Teil lautet, „Es ist verboten, Bürger auf irgendwelche Art und Weise zu beleidigen, zu verleumden, anzuschwärzen und hereinzulegen“. Das hat den Inhalt über Gewährleistung eines einzelnen Rechts zum Ausdruck gebracht. Im Großen und Ganzen entspricht dies dem verfassungsmäßigen Persönlichkeitsrecht. Siehe Lin Laifan und Luo Zhen-gyan: „Das verfassungsmäßige Persönlichkeitsrecht“, in „Juristen“ 2008, 5. Ausgabe

haben. Bei unterschiedlichen Rechtsbündeln können Datenvermögenswerte auch unterschiedlich sein (siehe Abbildung 2-1).

2. Zusammenstellung der gesetzlichen Interessen von Datenrechten

„Rechte sind Bedeutungskraft, die einer Person durch gesetzliche Vorschriften zur Erfüllung ihrer persönlichen Interessen gewährt wird, d.h. die Rechtskraft für die Person, bestimmte Interessen zu genießen“ (Hans Brox & Wolf-Dietrich Walker 2019, S. 276). Das Recht ist die ausgereifteste Kategorie im Rechtssystem. Es zeigt zutiefst den internen Zusammenhang zwischen den Rechten und tatsächlichen Interessen (Lü Zhixiang & Zhang Qiang 2019). Die Änderung des Status der Rechte zeigt, dass die Entwicklung der derzeitigen Beziehungen zwischen dem Staat und Individuum immer mehr von Rechten geleitet wird. Nach der klassischen westlichen Rechtstheorie beziehen sich Rechte im abstrakten Sinne auf Freiheit, Interessen und Gerechtigkeit, und man kann sogar mit Sicherheit sagen, dass private Rechte einfach gleich Freiheit, Interessen und Gerechtigkeit sind. Unter privaten Rechten werden individuelle Rechte verstanden, die auf die Befriedigung individueller Bedürfnisse abzielen und sich auf die Verkörperung und Wahrung persönlicher Interessen konzentrieren. Dieses „Individuum“ ist im Grunde privater Natur. Daher sind „Datenrechte aus Sicht der privaten Rechte die Rechte von Unternehmen, anderen Organisationen und Bürgern, die ihnen zugeordneten Daten und die von ihnen erfassten Daten zu besitzen“ (Lü Tingjun 2017).

Im letzten halben Jahrhundert ist die Gesetzgebung zum Schutz persönlicher Daten zu einer der bemerkenswertesten Gesetzgebungsbebewegungen der Welt geworden. Für den Schutz und die Nutzung personenbezogener Daten verfolgen viele Länder einen zweigleisigen Vorgang der Regulierung durch das öffentliche Recht und der Ermächtigung durch das Privatrecht (Cheng Xiao 2018). Das vom Bundesland Hessen (Deutschland) im Jahre 1970 verabschiedete „Datenschutzgesetz“ ist das erste spezielle Schutzgesetz für persönliche Daten der Welt. Dazu wurde ein Datenschutzausschuss eingesetzt, der die Speicherung und Übermittlung von amtlichen Dokumenten der Landesregierung überwachen soll,

um die illegale Erfassung, Revision und Zerstörung zu verhindern. 1973 verabschiedete Schweden zum Zwecke des Schutzes personenbezogener Daten das „Datenschutzgesetz“, das das erste Gesetz der Welt war, das die grenzüberschreitende Übermittlung personenbezogener Daten ausdrücklich einschränkte. 1974 begann der Kongress der Vereinigten Staaten angesichts des schweren Missbrauchs personenbezogener Daten den Schutz personenbezogener Daten zu erwägen und schließlich wurde das Datenschutzgesetz „Gesetzesvorlage für Privatsphäre“ verabschiedet. In Bezug auf die regionale oder globale Zusammenarbeit hat die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) im Jahre 1980 die „Leitlinien zum Schutz der Privatsphäre und der grenzüberschreitenden Verkehr personenbezogener Daten“ auf der Grundlage der Koordination und Vereinheitlichung verschiedener nationaler Gesetze in Bezug auf Datenschutz herausgegeben. Das Ziel war es, Empfehlungen für den Schutz der Privatsphäre und Freiheit der personenbezogenen Daten zu geben. In den 70er-Jahren des 20. Jahrhunderts begann die Europäische Union, ihre Mitgliedstaaten aufzufordern, Rechtsvorschriften über Daten zu erlassen, und setzte die legislative Arbeit zum Schutz personenbezogener Daten mit stetigen Fortschritten der Technologie und Gesellschaft kontinuierlich fort. Insbesondere definiert erneut die in 2018 eingeführte „Allgemeine Datenschutzverordnung“ den Inhalt wie die Berechtigung für personenbezogene Daten und Gewährung den Dateninhabern das Recht, ihre eigenen Daten zu vergessen und zu löschen.

Das System der persönlichen Datenrechte ist eine theoretische Antwort auf reale Ansprüche, sodass es zwangsläufig von den „gebührenden Rechten“ zu den „gesetzlich anerkannten Rechten“ und dann zu den „realen Rechten“ gehen muss (Shi Pengpeng 2013). Der Übergang des Systems der personenbezogenen Datenrechte von den gebührenden Rechten zu den realen Rechten hängt tatsächlich davon ab, dass die günstige Beeinflussung der gebührenden Rechte an Einzelfällen das Selbstbewusstsein der individuellen Inhaber für sein Recht aufgerufen hat und dann zu einem Konsens über Rechtsansprüche der überwiegenden Mehrheit der Gesellschaft entwickelt. Auf dieser Grundlage ist es notwendig, diese Rechtsansprüche in Form von Rechtsvorschriften festzulegen und diese mit entsprechender institutioneller Anordnung zu

bestätigen (Wen Yu 2019). Mit dem Fortschreiten des Datenisierungsprozesses wurden die diesbezüglichen Regeln des Schutzes personenbezogener Daten in grundlegende und wichtige Gesetze unseres Landes wie die Änderung des „Strafrechts“, Änderung des „Gesetzes für Schutz der Rechte und Interessen der Verbraucher“ und das „Cybersicherheits-Gesetz“ usw. eingeführt. Der Artikel 111 der „allgemeinen Bestimmungen des Zivilrechts“, das die grundlegende Stellung im Bereich des Schutzes der privaten Daten besitzt, hat zum ersten Mal das Recht der natürlichen Personen für Schutz persönlicher Informationen in allgemeiner gesetzlicher Form festgesetzt und den legalen Grundsatz für Erfassung und Verwendung persönlicher Informationen hervorgehoben. Dass die Rechte auf Schutz persönlicher Informationen oder Daten in die „allgemeinen Bestimmungen des Zivilrechts“ aufgenommen worden sind, ist von großer Bedeutung.

3. Sozialer Kontext der Datenrechte

Das Verständnis der Datenrechte und -interessen kann sich von der richtigen Erfassung der gegenwärtigen gesellschaftlichen Bedingungen im In- und Ausland nicht trennen. In den letzten Jahren haben sich Internetbenutzer auf der ganzen Welt mit dem faustischen Handel mit großen Unternehmen der Wissenschaft und Technologie beschäftigt:² Sie übermitteln ihre personenbezogenen Daten und erhalten Dienstleistungen. Lange Zeit sind sich die meisten Internetbenutzer nur der oberflächlichen Bedeutung bewusst, dass sie kostenlose Dienstleistung erhalten, vernachlässigen aber die tief gehende Bedeutung, dass Technologieunternehmen auch ihre persönlichen Daten kostenlos erfassen und benutzen. Diese persönlichen Daten werden nicht nur bewusst kommerziell genutzt, sondern auch mehrfach weitergegeben, gehandelt und missbraucht (Xi Po 2018). Zahlreiche Rechtsfälle haben gezeigt, dass

2 Der faustische Handel ist ein psychisches Hindernis, dessen Hauptinhalt lautet: Wenn ein Mensch ein wahrscheinlich wertvollstes Ding so blind verehrt, könnte er dazu geführt werden, den Grund und Gelegenheit zu verlieren, um andere wertvolle Dinge oder Geiste zu verstehen.

Daten zu Objekt des Rechts werden können. Es gibt viele solche Fälle im Ausland: Zum Beispiel Verletzung der Privatsphäre bei Google Street View 2007, Sony im Diebstahl von Spieldaten in 2011, der PRISM-Vorfall von 2013, Datenleckage von drei großen Kreditkartenunternehmen in Südkorea 2014, Anthem Diebstahl von 80 Millionen personenbezogener Daten in 2015, die Auslagerung von bürgerlichen Informationen und Daten in der Türkei 2016, Verkauf von G-Mail (Google Mailbox) und Yahoos Konten in 2017, der Facebook Cambridge Analyse Vorfall von 2018 und das Feilbieten der Daten von 159 Millionen Nutzern von LinkedIn 2019 (siehe Tabelle 2-2) usw. In China gibt es auch eine Reihe von „Fällen der Datenleckage“, die durch E-Commerce-Plattformen, Portalwebsites und Internet-**Finanzierungsplattformen** verursacht worden sind, einschließlich sowohl der Leckage von E-Mail-Konten und Passwörtern als auch der Bankkarteninformationen. Die Menschen sind sehr besorgt über solche Fälle wie Verrat, Verkauf und Missbrauch von Daten etc.

„Persönliche Daten in der digitalen Ära werden nicht nur als wichtiger Produktionsfaktor angesehen, sondern auch als ‚Währung auf dem digitalen Markt‘ betrachtet“.³ Wir treten gerade in eine neue „Ära des Nutzungsrechts“ ein, die auf der Idee der Teilhabe beruht. Kevin Kelly, ein Technologie-Denker, wies klar und eindeutig darauf hin: „Ich kann für sie (Güter oder Dienstleistungen) bezahlen, aber ich kann sie nicht haben. In gewissem Maße ist das Nutzungsrecht auch zum Eigentumsrecht geworden“ (Kevin Kelly 2012, S. 111). Dasselbe gilt auch für Daten. Aber die uneingeschränkte Nutzung von Daten würde das ordnungsmäßige Leben zerstören, das die Menschheit gemeinsam lebt. Insbesondere in der modernen Gesellschaft, die durch die Anwendung von Big-Data-Technologien repräsentiert wird, haben die von Menschen verursachten Risiken die natürlichen Risiken als die wichtigsten Bedrohungen für das menschliche Überleben allmählich ersetzt. Wie man

3 Auf der „Konferenz für Digital Leben und Design-Innovation“ 2012 sagte Viviane Reding, Beauftragter für Justiz, Grundrecht und bürgerliche Angelegenheiten der EU, dass die persönlichen Daten zu „Währung auf dem heutigen Digitalmarkt“ geworden sind.

Tabelle 2-2 Typische Datensicherheitsvorfälle im Ausland

Zeit	Typischer Fall	Beschreibung
2007	Verletzung der Privatsphäre von Google Street View	Google sah sich einer Reihe von datenschutzrechtlichen Klagen gegenüber, weil Autos und Lastkraftwagen illegal zum Sammeln persönlicher Informationen wie E-Mails und Passwörter aus unverschlüsselten privaten drahtlosen Netzwerken verwendet wurden. Zu einer Zeit waren diese Klagen die größten ihrer Art in der amerikanischen Geschichte. Google hat Milliarden von Dollar verloren.
2011	Diebstahl von Sony-Spieldaten	Das PlayStation Game Network (PSN) der Sony Corporation, Japan, wurde gehackt und Daten von 77 Millionen Online-Spielbenutzern wurden gestohlen, einschließlich der Namen der Benutzer, Wohnadressen, E-Mail-Adressen, Geburtstage, Passwörter, Passwortabfragen usw. Es wurde der schwerste Hack und Datendiebstahl zu diesem Zeitpunkt.
2013	PRISM	Edward Snowden, ein ehemaliger Mitarbeiter der National Security Agency (NSA) der Vereinigten Staaten, gab der britischen „The Guardian“ einige geheime Dokumente des PRISM-Überwachungsprogramms der Agentur bekannt. Es wurde berichtet, dass die NSA die Anrufprotokolle von Millionen von Benutzern überwachte. Das als PRISM bekannte geheime Überwachungsprogramm wurde 2007 von den Vereinigten Staaten ins Leben gerufen, mit dem die NSA direkt auf die zentralen Server von Internetunternehmen zugreifen konnte, um nach Daten zu suchen und Informationen zu sammeln. Neun internationale Internetgiganten, darunter Microsoft, Yahoo! Google und Apple usw., wurden von dem Programm abgedeckt.

Tabelle 2-2 Fortsetzung

Zeit	Typischer Fall	Beschreibung
2014	Datenverlust von drei großen Kreditkartenunternehmen in Südkorea	Während der Entwicklung von Computerprogrammen, die von Kreditkartenunternehmen in Auftrag gegeben wurden, sammelten und enthüllten ein Mr. Park und andere Mitarbeiter von Rating-Unternehmen illegal 104 Millionen privaten Daten von Kunden, darunter sind KB-Karten, Lotte-Karten oder NH-Karten. Neben persönlichen Informationen wie Name, Telefonnummer, Wohnort und Firmenname handelte es sich um 5,391 vertrauliche Kreditinformationen wie ID-Kartenummer, Kredittransaktionsdetails und Steuerbefreiungsbescheinigungen für Kreditkartengenehmigungen, auf die mehr als die Hälfte entfiel die durchgesickerten Informationen. Dies ist der größte Vorfall, bei dem Kreditkarteninhaber in Südkorea ihre privaten Daten verloren.
2015	Anthem-Diebstahl von 80 Millionen persönlichen Informationen	Hacker haben achtzig Millionen Kundeninformationen von Anthem, einer US-amerikanischen Krankenkasse, gestohlen, darunter Name, Geburtsdatum, Informationen zu Gesundheitskarten, Sozialversicherungsnummern, Adressen, E-Mail-Adressen und Beschäftigungsinformationen (einschließlich Einkommen). Damit ist es das größte Leckage-Ereignis von Gesundheitseinrichtungen in den Vereinigten Staaten.
2016	Verlust persönlicher Informationen in der Türkei	Fast 50 Millionen persönliche Informationen türkischer Bürger waren betroffen, darunter eine Reihe sensibler Informationen wie Namen, ID-Kartenummern, Namen und Adressen der Eltern, die von Hackern mit einer IP-Adresse in Finnland gepackt werden. Menschen können die Daten, die sie interessieren, auf P2P-Weise beliebig herunterladen.

(Fortsetzung)

Tabelle 2-2 Fortsetzung

Zeit	Typischer Fall	Beschreibung
2017	Verkauf von G-Mail (Google-Mailbox) und Yahoo-Konto	Eine große Anzahl von G-Mail-Konten, Yahoo-Konten und PlayStation Netzwerkkonten und Passwörter wurden von einem Lieferanten mit dem Namen suntzu583 öffentlich im dunklen Web verkauft. Die Gesamtzahl der verkauften G-Mail-Konten betrug 4,928,888, die in drei Teile unterteilt war und jeweils Informationen über 2,262,444-Konten enthielt, einschließlich E-Mail-Adressen und Passwörter.
2018	Vorfall Facebook Cambridge Analyse	Cambridge Analysis, ein Datenanalyseunternehmen, das US-Präsident Donald Trump während der Präsidentschaftskampagne 2016 Datenanalyseedienste zur Verfügung stellte, und seine Tochtergesellschaft Strategic Communications Lab haben 50 Millionen Facebook-Nutzerdaten gestohlen und privat aufbewahrt, mit denen sie die Präsidentschaftswahlen manipuliert haben.
2019	Verkauf der Daten von 159 Millionen Nutzern von LinkedIn	Andrew, ein Hacker, hat sensible Daten von 159 Millionen Nutzern von LinkedIn auf Website Pastebin zum Verkauf angeboten. Um die Authentizität der Daten zu beweisen, hat der Hacker auch die Anmeldeinformationen von 100 Benutzern veröffentlicht, darunter auch Anmeldeinformationen von bekannten CEOs.

Risiken kontrolliert und Sicherheit sicherstellt, ist zu einem Thema geworden, das für die Entwicklung der modernen Gesellschaft von gemeinsamem Interesse ist. Wir müssen dringend einen Interessenausgleichsmechanismus einer neuen sozialen Ordnung schaffen, um die Unordnung zu bekämpfen, die durch Vernachlässigung der Rechte der Dateninhaber verursacht wurde.

Da die Menschen sich in unterschiedlichen Sozialszenarien befinden, unterscheiden sich die Ansprüche der Dateninhaber auf ihre eigenen Dateninteressen erheblich. Eine solche Interessendifferenzierung manifestiert sich vor allem in der Tatsache, dass einige Rechteinhaber erwarten,

personenbezogene Dateneigentumsinteressen, Datenpersönlichkeitsinteressen und Privatsphäre-Datenschutzinteressen zu erhalten und sogar den Zweck verfolgen, die öffentliche Macht des Staates einzuschränken, indem sie Rechte auf persönliche Daten beanspruchen. Die Verwirklichung persönlicher Interessen erfordert jedoch den Verbrauch sozialer Ressourcen, während persönliche Interessen nur erreicht werden können, wenn soziale Interessen gewahrt werden. Daher hängt die Verwirklichung von persönlichem Datenrecht in der Regel stark von der Verwirklichung sozialer Interessen ab. Im Prozess der Gesetzgebung zum Schutz persönlicher Daten sollte Wertausrichtung genommen werden, d.h. soziale Interessen haben Vorrang vor persönlichem Datenrecht. Für soziale Interessen ist die Priorität für verschiedene soziale Gruppen jedoch auch unterschiedlich. Selbst wenn es notwendig ist, soziale Interessen durch Einschränkung der persönlichen Datenrechte zu schützen, sollten solche Einschränkungen auch angemessenen „Grad“ einhalten und einigen Grundprinzipien folgen (Wang Xiuxiu 2018, S. 143–172).

(III) *Datenmacht*

I. Übergabe der Macht

Die Macht ist in der Natur öffentliche Macht. Sie stellt eine Art soziale Beziehungen zwischen Menschen dar und existiert in einer dynamischen Bewegung (Jiao Shiwen 2009, S. 21). Sie ist immer „der offizielle Vertreter der gesamten Gesellschaft und eine kollektive Verkörperung der Gesellschaft in einer konkreten Organisation“ (Central Compilation and Translation Bureau 1963, S. 242). Die öffentliche Macht ist dem Wesen nach auch eine Art Recht, aber sie ist eine besondere Art von Rechten. Die Staatsmacht ist die Manifestationsform der staatlichen Rechte. Als Hauptsymbol des Staates ist sie die Grundvoraussetzung für alle funktionalen Tätigkeiten des Staates. Sie hat drei grundlegende Merkmale: Erstens ist das Subjekt der öffentlichen Macht eher die breite Öffentlichkeit als die Einzelperson, und die Öffentlichkeit ist der Kerninhalt der öffentlichen Macht. Die öffentliche Macht verkörpert die

Gemeinschaftlichkeit, Gemeinnützlichkei und Gemeinsamkeit. Zweitens sollte sich das Objekt der öffentlichen Macht auf öffentliche Angelegenheiten beziehen, während anderes, was private Rechte betrifft, nicht durch die öffentliche Macht gestört werden sollte. Andernfalls handelte es sich um eine Verletzung der privaten Rechte. Drittens sind öffentliche Interessen die Quelle und das Fundament der öffentlichen Macht. Die öffentliche Macht sollte die öffentliche Verantwortung tragen und den öffentlichen Interessen dienen. Sonst würde sie möglicherweise privatisiert oder sich in Privatbesitz geriete (Hao Jiming 2008).

In einem Bericht der Vereinten Nationen wurde darauf hingewiesen: „Daten sollen darauf abzielen, die soziale Existenz zu rationieren und eine ‚rationale Produktion‘ der Begriffe und Bedeutungssysteme zu verwirklichen. Eben deshalb sind Daten derzeit und in Zukunft eine wichtige strategische Ressource“. Diese strategische Ressource ist im Wesentlichen die Datenmacht. Die Datenmacht ist eine moderne Macht, während die Datenmacht eine dyadische Macht, die die Rationalität dominiert und wiederum von ihr dominiert wird. Mit Blickwinkel der politologischen Theorie folgt die Datenmacht der Logik der Macht, die die Fähigkeitslogik und Strukturlogik beinhaltet und neue politische, wirtschaftliche und soziale Beziehungen ständig produziert, formt und dominiert. Die Fähigkeitslogik spiegelt die Dimension der Natur der Rolle, der Objektivität und der Technologie wider, während die Strukturlogik die Dimension ihrer Beziehungsfähigkeit, Regelmäßigkeit und Musterhaftigkeit darstellt. Diese beiden logischen Kategorien enthalten sowohl positive endogene Triebkraft, könnten jedoch aufgrund ihrer brandender Auswirkungen auf das bestehende soziale Machtssystem auch zu Risiko-Disgruent und Konflikt zwischen öffentlichem und privatem Bereich führen. Daher müssen wir einen rationalen und umsichtigen Konsens für die Datenmacht schmieden und eine Idee für Datenverwaltung hervorbringen.

Daten sind wie Wissen auch die „demokratischste Machtquelle“. Mit der Entwicklung der Datenmacht wandelt und verlagert sich auch die traditionelle Macht um. Erstens befindet sich das Machtzentrum der Welt zurzeit in einer regionalen Verlagerung. Angetrieben von digitaler Technologie entwickeln sich Schwellenländer wie China und Indien rasant und ihre umfassende nationale Stärke, ihr internationaler Einfluss und ihr

Diskursrecht nehmen zu, während die Vereinigten Staaten und die Europäische Union in der Zwischenzeit gruppenweise relativ herunterkommen und das Machtzentrum der Welt verlagert sich somit nach Osten. Zweitens bewegt sich die Macht von der oberen zur niedrigen Ebene und breitet sich allmählich auf die Mehrheit der Menschen aus. In wissensintensiven Unternehmen haben Manager, technische Experten und Arbeitnehmer mehr Macht, was beweist, dass „Wissen die demokratischste Machtquelle ist“. Drittens ist die Umwandlung der Macht von der minderqualitativen in die hochqualitative Ebene. Im Zeitalter der digitalen Wirtschaft sind Daten die Hauptmacht. Sie verfügt über Fähigkeit und Funktion, das Antlitz der Welt und der Gesellschaft zu verändern, über die die Gewalt und der Reichtum niemals verfügt haben könnten. Viertens entsteht ein neues Machtzentrum, das Daten als Ermessungskriterien genommen hat. Diejenigen Datenschichten, die Informationsintelligenz, das neueste technologische Know-how und wichtige Datenressourcen beherrschen, werden zum Machtzentrum.⁴

2. Expansion der Datenmacht

Daten sind Macht und Macht ist Daten. Macht kann in Daten umgewandelt werden. Daten sind zu einer unverzichtbaren Macht geworden. In gewissem Sinne kann man sogar sagen, dass diejenigen die Macht haben, die Daten besitzen. Ein neues Machtsystem – Datensystem – kommt gerade auf. Die Datenmacht hat die traditionelle gegensätzliche

4 1990 wies Alvin Toffler in „Powershift“ darauf hin, dass Macht als Kraft, andere zu dominieren, seit der Antike durch Gewalt, Reichtum und Wissen verwirklicht wurde. In der dritten Welle der Zivilisation wird Wissen zum Symbol der Macht. Wer Wissen hat, wird Macht haben. Wissen unterscheidet sich jedoch von Gewalt und Reichtum darin, dass die beiden Letzteren exklusiv sind. Wenn eine Art von Gewalt oder Reichtum einer Person oder Gruppe gehört, können andere Personen oder Gruppen die Gewalt oder den Reichtum nicht gleichzeitig besitzen, während Wissen nicht exklusiv ist und dieselbe Art von Wissen gleichzeitig verschiedenen Menschen gehören kann. Daher ist „Wissen die demokratischste Machtquelle“. Wer das Kontroll- und Verbreitungsrecht des Wissens hat, hat die Initiative der Macht. Im Zeitalter von Big Data wird jedes „Rechenzentrum“ in gewissem Sinne zu einer Art „Rechts-/Machtzentrum“, und diese „Rechts-/Machtzentren“ haben Diskursrechte.

Dualstruktur von Staat und Gesellschaft verändert und ein neues Muster des komplexen Wettbewerbs zwischen öffentlicher Macht und privaten Rechten gebildet. Öffentliche Datenmacht und private Datenrechte sind eine dialektische Einheit der Gegensätze. Unter bestimmten Bedingungen bilden die öffentliche Macht des Staates und die privaten Rechte der Gesellschaft eine gewisse Koalition für die Regierungsführung, um die Ausweitung der sozialen privaten Rechte zu verhindern. In ähnlicher Weise kooperieren private Rechte in der Regel auf der Grundlage einschlägiger Rechtsansprüche und Bestrebungen, um die Ausweitung und den Missbrauch öffentlicher Macht gemeinsam einzudämmen.

Im Zeitalter von Big Data erstreckt sich der Anwendungsbereich der Macht von den ursprünglichen politischen und rechtlichen Bereichen auf alle Aspekte des sozialen Lebens wie Geschäft, medizinische Versorgung, Bildung und Kultur etc., was zweifellos den Raum der Datenmachtinhaber für ihre Machtausübung erweitert. Dies macht es einfacher, Macht in Verkleidung zu missbrauchen, was aber dazu führt, dass die Datenmacht noch schwer zu kontrollieren ist. „Als Knotenpunkt zwischen Rechteinhabern im Cyberspace und in der realen Welt sammeln Kontos durch verschiedene Online-Aktivitäten Daten stetig an, während sie diese auf der Basis der Beurteilung ihrer Szenarien-Handlungen wiederum zu wichtiger Einschränkungskraft für Einfluss auf ihre zukünftigen Aktivitäten der Kontoinhaber machen“ (Hu Ling 2018). In diesem Prozess kann man nicht an der Erfassung und Verwendung seiner Daten durch andere Personen teilnehmen und diese in der Hand haben. Er kann gar nicht die Benutzung der außer Kontrolle gekommenen persönlichen Daten kontrollieren. Auch wenn kein Geheimnis gelüftet würde und niemand zusähe, könnte sein Recht auf Datenprivatsphäre bereits in gewissem Sinne verletzt. Diese Art von Sorge und Angst ist besorgniserregender als die direkte Verletzung der Macht.

Da die Macht dezentralisiert und auf niedriger Ebene verteilt wird, sind jetzt mehr Menschen darüber informiert und haben auch Beteiligungsrecht bekommen, während dies aber auch neue Probleme der Machteinschränkung mit sich bringt. Mit der Machtverlagerung ändert sich auch die Macht der Regierung. Es entsteht eine Art dezentrale und diversifizierte Demokratie, die einen wichtigen Einfluss auf die Verhinderung der

übermäßigen Machtkonzentration und dadurch entstandene Korruption in der Regierungsführung hat. Vor diesem Hintergrund „könnte eine Form der Macht zerstört werden, eine andere ersetzt sie aber gerade“ (Hu Ling 2018). Das bedeutet, dass der strukturelle Wandel hin zu einer pluralistischen Verwaltung im Zeitalter von Big Data zu tief greifenden Veränderungen der Rechtsbeziehungen führen kann. Es ist notwendig, entsprechende Gesetze und rechtliche Vorschriften in Bereichen, in denen ein Missbrauch der Datenmacht möglich ist, zu erstellen.

3. Struktur der Datenmacht

„Macht kommt von der sozialen Struktur. Eine bestimmte Macht kommt aus einer bestimmten Position in der sozialen Struktur“ (Kang Xiaoguang 1999, S. 51). Die soziale Struktur ist Basis für Existenz einer Machtstruktur. Jede soziale Struktur hat zwangsläufig ihre entsprechende Machtstruktur. Die strukturelle Logik der Datenmacht ist das Produkt unseres Engagements für die Selbstentwicklung und Aufrechterhaltung des modernen Zivilisationssystems (Lin Qifu & He Jingchao 2016). Die politische und soziale Struktur der Datenmacht dient als öffentliches System der Datenmachtstruktur im öffentlichen Sinne. Das erläutert, was für Struktur der öffentlichen Ordnung die Datenmacht erzeugen kann. Ihre Funktionen werden hauptsächlich in den sozialen Praktiken der Politik sowohl auf dem Mikro- als auch Makrogebiet gesehen. Es ist eine staatliche Handlung, bei der das kompetente Subjekt der Datenmacht sie durch verschiedene praktische Prozesse wie soziale Kontrolle, Mobilisierung, Überzeugung, Absorption und sogar Zeichenproduktion usw. mit verschiedenen Ressourcen aufgebaut hat. In wirtschaftlicher Hinsicht entwickelt sich die Datenmacht entlang des Zyklus von Keimung – Bildung – Reife – Stagnation – Rezession – Spaltung – Keimung, der die Geschichte der Änderung der sozialwirtschaftlichen Formen und Regeln umreißt. Das Aufkommen von Datenmacht bietet sowohl Wahrscheinlichkeit als auch Unsicherheiten für diesen Zyklus. Die Datenmacht wird die bestehende Marktstruktur infrage stellen, Einfluss auf den Wettbewerb um Kapital nehmen und eine sozialisierte Umverteilung der Mikro Eigentumsrechte bewirken. Die konzeptionelle Lebensstruktur der

Datenmacht ist ein einheitlicher Rahmen des Systems menschlicher Bedeutung und des kulturellen Systems. Im Vergleich mit den ersten beiden Strukturen ist sie jedoch noch vielfältiger und komplexer. Daten sind nicht mehr der Überschuss der Machtstruktur, sondern spielen mit Positur der Macht eine Rolle bei der Integration und Reorganisation der konzeptionellen Lebensstruktur. In Zukunft basiert die Identität der Menschen möglicherweise nicht mehr auf Blutverwandtschaft, ethnischer Gruppe, Familienname oder Herkunftsort. Stattdessen identifizieren sie sich miteinander mit der Datenidentität, Internet der Dinge-Wohnbezirk und Position im Cyberspace.

Abschnitt II Type der Datenrechte

Die gesetzliche Bestätigung von Datenrechten ist sowohl Grundlage für Rechtsausübung und Rechtsschutz, sondern auch ein wichtiges Mittel für Interessenschutz. „Die datenbezogenen Interessentinhaber sind Einzelperson, Unternehmen, andere Organisationen und Länder. Kategorie und Eigenschaft der Datenrechte und -interessen, die verschiedene Interessenssubjekte besitzen, ist auch unterschiedlich“ (Li Xiaoyu 2019). Die Entwicklung der Big-Data-Industrie hat entsprechende neue Rechts- und Interessenssubjekte hervorgebracht, w. z. B. Dateninhaber, Datenkontrolleur und Datenbenutzer etc. In Bezug auf Datenrechtssubjekt umfassen Typen der Datenrechte persönliches Datenrecht, Unternehmensdatenrecht und Regierungsdatenrecht. „Sobald die Rechte gesetzlich festgelegt sind, besteht die erste Frage darin, seine Funktionsstruktur zu entwerfen. Die konkrete Wirkungsform der Funktionalität stellt die gesetzliche Anerkennung von Rechtsposten dar“ (Chen Zhentao 2017). Angetrieben durch Interessen werden verschiedene Interessenssubjekte unweigerlich neue Ansprüche zum Schutz der einschlägigen Rechte und Interessen und des entsprechenden Rechtssystems geltend machen. Infolgedessen können Daten nur dann umfassender geschützt werden, wenn eine eingehende Untersuchung der Theorie über Datenrechte und Festlegung der Funktionsstruktur erfolgt.

(I) Rechte an personenbezogenen Daten

1. Personenbezogene Daten

Im Zeitalter von Big Data haben Daten und ihre Derivate einen ständigen Einfluss auf das persönliche Leben. Informationen über alle Aspekte von Menschen als Individuen werden in Form von Daten gesammelt, aussortiert und verwendet (Li Xiaoyu 2019). Massive personenbezogene Daten enthalten einen enormen wirtschaftlichen und strategischen Wert. Einerseits nießbrauchen Benutzer durch Verwendung personenbezogener Daten und ständige Verbesserung der Technologie und Funktionen von Datenprodukten mehr Vorteile und Komfort, die die Entwicklung der Daten gebracht worden sind. Auf der anderen Seite ist jeder das Subjekt der Datenquelle. Wenn personenbezogene Daten nicht ausreichend geschützt werden könnten, könnte dies zu Problemen wie illegale Erhebung, Verkauf und Verwendung personenbezogener Daten sowie Verletzung der Persönlichkeitsrechte und Eigentumsrechte von Einzelpersonen führen. Wenn personenbezogene Daten kommerziell genutzt werden, wird ihr kommerzieller Wert aufgrund der damit verbundenen Persönlichkeitsinteressen mittelbar aktiviert. Man kann sagen, dass die Rechtsvereinbarung für personenbezogene Daten direkt bestimmt, wie Daten zirkulieren und wie sie gemein genutzt werden, was wiederum einen großen Einfluss auf die Entwicklung der Datenbranche übt.

Personenbezogene Daten sind auch als persönliche Informationen oder persönliche Unterlagen genannt.⁵ Zum Beispiel hat die Europäische Union in der „Datenschutzgrundverordnung“ vorgeschrieben: „Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen.

5 Es gibt verschiedene Bezeichnungen, die sich auf personenbezogene Daten beziehen, wie z. B. „personenbezogene Daten“, „persönliche Informationen“ usw. Der Unterschied beruht jedoch hauptsächlich auf unterschiedlichen Rechtstraditionen und Nutzungsgewohnheiten. Es gibt keine wesentlichen Unterschiede. In der Big-Data-Technologie liegen Informationen meist in Form von Daten vor, daher werden sie hier als „personenbezogene Daten“ bezeichnet.

Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere unter Bezugnahme auf ein Kennzeichen wie Namen, Identifikationsnummer, Standortdaten, Online-Kennung oder auf einen oder mehrere physikalische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person“.⁶ Nach dem japanischen „Gesetz zum Schutz personenbezogener Daten“ bezeichnet der Begriff „personenbezogene Daten“ Informationen über eine bestimmte Person, die diese Person anhand ihres Namens, ihres Geburtsdatums oder einer anderen Beschreibung identifizieren können, einschließlich solcher Informationen, die einen einfachen Verweis auf andere Informationen ermöglichen und dadurch die Identifizierung des spezifischen Individuums ermöglicht wird (Wen Yu 2018). Im Cybersicherheitsgesetz der Volksrepublik China wird definiert: „Persönliche Informationen beziehen sich auf alle Arten von Informationen, die elektronisch oder auf andere Weise aufgezeichnet werden und allein oder zusammen mit anderen Informationen ausreichen, um die Identität einer natürlichen Person zu identifizieren, einschließlich, aber nicht beschränkt auf die vollständigen Namen, Geburtsdaten, nationale Identifikationsnummern, persönliche biometrische Informationen, Adressen, Telefonnummern usw.“⁷ Der Hauptstrom in der akademischen Gemeinschaft ist der Ansicht, dass der essentielle Standard für Identifizierung personenbezogener Daten die „Identifizierbarkeit“ ist. „Personenbezogene Daten können sich auf eine bestimmte Person beziehen, und ihre Verarbeitung kann das Leben dieser natürlichen Person beeinträchtigen oder sogar schädigen, mit der sie verbunden sind. Das ist eben der Grund dafür, weshalb personenbezogene Daten geschützt werden müssen“ (Wen Yu 2019).

„Das Recht auf personenbezogene Daten beinhaltet die Koordination zwischen dem Schutz der Bürgerrechte und Interessen natürlicher Personen und der Freiheit der Datenunternehmen, datenbezogene Aktivitäten durchzuführen“ (Cheng Xiao 2018). „Das Recht auf personenbezogene

6 Siehe EU-Datenschutzgrundverordnung, Art. 4 Abs. 1 (DSGVD).

7 Siehe Art. 76 des „Cybersicherheitsgesetz der Volksrepublik China“

Daten ist das Recht der betroffenen Personen, zu entscheiden, wer und wie ihre personenbezogenen Daten erfasst, verarbeitet und analysiert, und es ist eine Art Kontrollrecht für personenbezogene Daten“ (Xiang Liling & Gao Qianyun 2018). Die Ansprüche der Einzelperson auf personenbezogenen Daten manifestieren sich in der Forderung, dass ihre Persönlichkeitsrechte und Eigentumsrechte an personenbezogenen Daten auf gesetzlicher Ebene nicht rechtswidrig verletzt werden. Insbesondere werden die neuen Arten von Rechten in Bezug auf Daten hauptsächlich wie folgt dargestellt: Zusätzlich zu dem durch bestehende Gesetze anerkannten Recht auf Privatsphäre beanspruchen Internetnutzer auch das Recht auf Selbstbestimmung über personenbezogene Daten, das Recht, personenbezogene Daten mitzunehmen, das Recht auf Vergessen ihrer personenbezogenen Daten, das Recht auf Übermittlung personenbezogener Daten und das Recht auf ausschließlichen Zugriff auf personenbezogene Daten (siehe Tabelle 2-3). Es ist ersichtlich, dass „Datenrechte und -interessen kein einziges Recht, sondern ein Bündel verschiedener Rechte sind“ (Li Xiaoyu 2019).

2. Rechte an persönlichen Daten: Eine neue Art von Persönlichkeitsrecht

Die Daten beinhalten die Nutzungsgewohnheiten, Lebensbedingungen, Kommunikationsprivatsphäre und andere Informationen eines Benutzers, mit denen die Person identifiziert werden kann, einschließlich der zu schützenden Informationen des Persönlichkeitsrechts wie Namens- und Porträtrechts des Einzelnen usw. Aufgrund der Identifikationsmerkmale und Identifikationsvorteile enthalten die Datenrechte zweifellos Persönlichkeitsrechte (Yan Lidong 2019). Die personenbezogenen Daten, die anonym verarbeitet sind oder nur geringe Empfindlichkeit aufweisen, wie zum Beispiel Informationsdaten wie Aufzeichnungen zum Surfen im Internet und persönliche Konsumgewohnheiten, sind jedoch nicht unbedingt mit der Persönlichkeit und Identität der betroffenen Personen verbunden und gelten daher auch nicht für Anspruch der Privatsphäre wegen Verletzung des Persönlichkeitsrechts. Darüber hinaus ist es im Hinblick auf Abhilfemaßnahmen

Tabelle 2-3 das System der Rechte an personenbezogenen Daten

Recht	Beschreibung
Recht auf Privatsphäre	Die Datenprivatsphäre betrifft nicht nur die persönliche Identifizierung, sondern auch die Verhaltensspur einer Person, die Konsumtendenz, Gewohnheiten und andere verwandte Informationen etc. Es wurde weltweit anerkannt, dass das Recht auf Datenprivatsphäre hauptsächlich bedeutet, dass man das Recht hat, seine privaten Informationen nicht illegal weitergegeben werden, anstatt sie zu beherrschen oder zu kontrollieren.
Recht auf Information	Das Recht auf Information, auch als Recht auf Selbstbestimmung von Informationen bekannt, ist das Recht, die Datenverarbeitung einzuschränken. Es betont die Kontrolle persönlicher Informationen, einschließlich nicht nur der Aktualisierung und Löschung der Informationen, sondern auch des Wissens des Zwecks, des Ziels und der Verwendung der Informationen.
Recht auf Wissen	Das Recht des Einzelnen zu wissen, wie seine Daten gesammelt und verwendet werden.
Recht auf Zugang	Dies bezieht sich auf das Recht auf Zugang zu persönlichen Daten. Die Allgemeine Datenschutzverordnung von EU sieht vor, dass die für die Verarbeitung Verantwortlichen entsprechende Verfahren zur Ausübung dieses Rechts durch die Benutzer vorsehen. Ein für die Datenverarbeitung Verantwortlicher kann keine Gebühren für die Bereitstellung dieses Dienstes erheben, es sei denn, die Anforderung der betroffenen Person scheint übermäßig zu sein.
Recht auf Widerspruch	Das Recht auf Widerspruch bezieht sich auf das Recht auf Verweigerung der Datenverarbeitung Verantwortlicher der Verarbeitung der persönlichen Daten auf der Grundlage seiner/ihrer legitimen Rechte und Interessen und das Recht auf Ablehnung von Marketinghandlung im Zusammenhang mit seiner/ihrer persönlichen Daten.
Recht auf Datenübertragbarkeit	Benutzer können ihre persönlichen Daten von einem Datenverantwortlichen auf einen anderen übertragen, ohne gestört zu werden.
Recht auf Berichtigung	Um die Richtigkeit der Daten zu gewährleisten, haben die betroffenen Personen das Recht, die Daten zu korrigieren.

Tabelle 2-3 Fortsetzung

Recht	Beschreibung
Recht auf Vergessenwerden	Wenn ein Benutzer die Einwilligung gemäß dem Gesetz widerruft oder der für die Verarbeitung Verantwortliche nicht mehr den berechtigten Grund hat, die Daten weiter zu verarbeiten, hat der Benutzer das Recht, die Löschung der Daten zu verlangen.

Quelle: Siehe Sun Wei: „Datenrechte, offener Mechanismus und Metadatenstandard in offenen Daten: Erfahrungen im globalen Bereich.“ Akademisches Komitee für Stadtverkehrsplanung der China Stadtplanungsgesellschaft. Die Theorien des innovativen Fortschritts und der Intelligenzentwicklung: Berichte der Jahreskonferenz der chinesischen Stadtverkehrsplanung, 2018.

aufgrund der Vertraulichkeit der Datenerfassung und -nutzung unmöglich, den Kausalzusammenhang zwischen dem, der die Daten gesammelt und verwendet hat, und dem aufgetretenen Verstoß nachzuweisen, was die Identifizierung des Verletzenden und Nachweisen der Verletzung sehr schwierig macht.

Da es sich bei Daten um eine neue Art von sozialen Ressourcen handelt, muss eine neue Art von Persönlichkeitsrechten eingeführt werden, um die Erhebung und Verwendung von Daten zu regeln und zu schützen. Erstens nehmen die Rechte der persönlichen Daten in Bezug auf die inhärenten Merkmale der Rechte die Persönlichkeitsinteressen als ihr Schutzobjekt, und die Datensubjekte haben die Rechtseigenschaft, ihre Daten zu kontrollieren und zu verfügen und so haben sie spezielle Rechtskonnotation. Zweitens umfassen die persönlichen Daten in Bezug auf die Vielfalt der Rechtsobjekte üblich persönliche Informationen, persönliche Geheimnisdaten und sensible personenbezogene Daten, unter denen einige auf bestimmte Persönlichkeitsrechte gestiegen haben, z. B. Name, Porträt und persönliche Geheimnisse etc. Außerdem unterliegt der ihnen gebotene Schutz in Bezug auf die Wirksamkeit des Schutzmechanismus Einschränkungen, wenn Rechte der persönlichen Daten nur als Eigentumsrecht definiert werden.

Im Gegenteil, wenn die Rechte der persönlichen Daten als eine neue Art von Persönlichkeitsrechten angesehen werden, kann garantiert werden, dass die Berechnungsmethode nicht infolge des Unterschiedes der persönlichen Identität auch unterschiedlich ist, damit der allgemeine Grundsatz der Persönlichkeitsgleichheit aufrechterhalten wird. „Die Schaffungsweise von einer neuen Art von Rechten kann die rechtlichen Beziehungen klar veranschaulichen, und diejenigen, die die entsprechenden rechtlichen Bestimmungen anwenden, können mittels Rechtsobjekte diese Bestimmungen eindeutig überprüfen“ (Zhang Suhua & Li Yanan 2018). Wie Professor Wang Liming sagte, „sollten die persönlichen Informationen als Objekt des Persönlichkeitsrechts privatrechtlich geschützt werden und ein spezielles Gesetz für den Schutz der persönlichen Informationen sollte formuliert werden“ (Wang Liming 2013). Im Zeitalter der digitalen Zivilisation sollten die Rechte der persönlichen Daten von Rechts wegen als ein neues eigenständiges Persönlichkeitsrecht verankert werden, deren Ziel ist, die Rechte und Interessen der Datensubjekte vor Verletzungen zu schützen und die persönlichen Daten nicht missbraucht und willkürlich verbreitet zu werden. Gegenwärtig ist das von Datenrechten betroffene Persönlichkeitsrecht ein gesetzlich festgelegtes Recht, das von Rechtstheoretikern und Praktikern schon anerkannt worden ist. In ähnlicher Weise wurde das Persönlichkeitsrecht bei der Formulierung des chinesischen Bürgerlichen Gesetzbuchs⁸ als ein separates Kapitel erstellt und der Schutz persönlicher Informationen im Schutz des Persönlichkeitsgesetzes

8 Am 22. August 2019 fand in Peking die 12. Sitzung des Ständigen Ausschusses des 13. Nationalen Volkskongresses statt. Auf dieser Sitzung wurde die dritte Lesung des Persönlichkeitsrechts des Bürgerlichen Gesetzbuchs (Entwurf) durchgeführt und die einschlägigen Bestimmungen zum Schutz personenbezogener Daten wurden vervollständigt. Darunter sind folgende neuen Bestimmungen hinzugefügt worden: Das Persönlichkeitsrecht ist das Recht des zivilen Subjekts auf Leben, Körper und Gesundheit, Name, Bezeichnung, Porträt, Ansehen, Ehre und Privatsphäre usw. Die Definition der Privatsphäre wurde wie folgend geändert: „privater Raum, private Aktivitäten und private Informationen usw., die natürliche Personen nicht wissen lassen möchten“. Die zusätzliche Bestimmung lautet, dass keine Organisation oder Einzelperson private Bereiche wie Hotelzimmer usw. anderer Personen durchsuchen, betreten, beobachten oder fotografieren darf.

aufgenommen. Dies ist eine Antwort auf die weitverbreitete Sorge der Gesellschaft vor den Herausforderungen, die die Entwicklung neuer Technologien mit sich gebracht hat.

3. Das persönliche Datenrecht als ein unabhängiges Eigentumsrecht

„Das Hervorkommen des potenziellen wirtschaftlichen Werts der persönlichen Daten macht es erforderlich, dass wir die in ihnen enthaltene Natur des Eigentums nicht ignorieren können und dass die Rechte der persönlichen Daten nicht nur als ein Objekt des Persönlichkeitsrechts geschützt werden können.“⁹ Dies würde der Datenfluss im Internet behindern und die Entwicklung der Big-Data-Branche zurückhalten. Darüber hinaus sind mit der umfassenden Verwendung und Verbreitung persönlicher Daten immer mehr wirtschaftliche Streitigkeiten aufgetreten, die den Eigentumscharakter persönlicher Daten immer wichtiger machten. Solche Streitigkeiten könnten nicht erfolgreich beigelegt werden, wenn das Recht der persönlichen Daten lediglich als ein einfaches Persönlichkeitsrecht behandelt würde. Insbesondere vor dem Hintergrund der digitalen Wirtschaft ist der wirtschaftliche Wert der persönlichen Daten noch offensichtlicher. Sollten Daten nur unter der Kategorie des Persönlichkeitsrechts geschützt werden, ginge es aber nur um das Rechtsobjekt in Bezug auf Persönlichkeit und Würde, was den Datenfluss und die Entwicklung der Datenbranche in gewissem Maße behindern könnte. Die Bestätigung des Eigentumsrechts von persönlichen Daten kann uns daher helfen, beidseitige Handlungen bei den Datentransaktionen besser zu regulieren, der Datenmarktstätigkeit ein gesetzmäßig geordnetes

9 Obwohl die in persönlichen Daten enthaltenen Persönlichkeitslemente die Eigenschaften von Persönlichkeitsinteressen und wirtschaftlichen Interessen aufweisen, können die Persönlichkeitsinteressen durch Berufung auf Persönlichkeitsrechte geschützt und die wirtschaftlichen Interessen der Datenpersönlichkeitslemente völlig als Vermögen verwirklicht werden. Zur „Vermögensorientierung von Datenpersönlichkeitslementen“ siehe Wen Yuheng: „Über die privatrechtliche Struktur des Dateneigentumsrechts“, Doktorarbeit; Xiangtan Universität, 2018.

Handelsumfeld zu geben und einen besseren Schutz der Rechte der persönlichen Daten zu gewähren.

Der Schutz der Datenrechte unterscheidet sich vom Schutz des Persönlichkeitsrechts, der Geschäftsgeheimnisse und des geistigen Eigentumsrechts usw. Es soll als ein eigenständiges Recht geschützt werden, das als Dateneigentumsrecht bezeichnet werden kann. Das Dateneigentumsrecht ist ein unvollständiges Eigentumsrecht. Der Inhaber oder Kontrolleur kann die von ihnen besitzenden oder kontrollierenden Daten weder willkürlich verfügen noch die legitimen Rechte und Interessen der relevanten Rechtsinhaber schädigen. Daher ist es notwendig, eine relevante Kategorisierung vorzunehmen und eine relevante Rechtssystemreihe basierend auf den Formen der Existenz von Informationen aufzubauen (Deng Ganghong 2018). Auf dieser Grundlage beziehen sich die persönlichen Datenrechte auf die unabhängigen Vermögensrechte des Datensubjekts im digitalen Zeitalter. Das Dateneigentumsrecht ist das Recht, mit dem der Rechtsinhaber ein bestimmtes Dateneigentum direkt zu verfügen und Störungen durch andere auszuschließen. Es ist eine neue Form des Eigentumsrechts, die im Zeitalter von Big Data geboren wurde. Zu seinen Funktionen gehört das Recht des Dateneigentümers, sein Dateneigentum zu besitzen, zu nutzen, zu verdienen und zu verfügen (Qi Aimin & Pan Jia 2015). Deshalb ist das Dateneigentumsrecht kein statisches Einwegrecht, sondern eine Gruppe von Eigentumsrechten.

Erstens besitzen personenbezogene Daten als Privateigentum des Datensubjekts Eigenschaft des materiellen Eigentums. Und ihr Wert kann in materielle Vorteile wie Geld usw. umgewandelt werden, die der Dateneigentümer oder -besitzer erhält. Zweitens ist das Recht der persönlichen Daten übertragbar. Der Dateneigentümer oder -besitzer kann sein Recht im gesetzlich zulässigen Umfang anderen Personen übereignen, damit die Daten vollständig verwandt werden. Drittens ist das rechtsbehelfsmäßig. Wenn das Recht des Datensubjekts verletzt wird, kann es die Verfügung über sein Recht der persönlichen Daten wieder erlangen oder Ersatz für den durch diese Verletzung verursachten Schaden gemäß den einschlägigen gesetzlichen Vorschriften beanspruchen. Daher kann das Recht der persönlichen Daten als unabhängiges Eigentumsrecht nicht nur den ordnungsgemäßen Betrieb der Datenbranche gemäß den gesetzlichen Bestimmungen

gewährleisten, sondern auch die Verwirklichung der Interessen des Datensubjekts und Datenkontrolleurs garantieren.

(II) Rechte an Unternehmensdaten

1. Unternehmensdaten

Im Zeitalter der digitalen Wirtschaft sind Daten in alle Bereiche unseres Lebens eingedrungen und zu einem wichtigen Produktionsfaktor und einem wichtigen Vermögen von Unternehmen geworden. Mithilfe von Daten können Unternehmen ihre Entscheidungsfindung, Innovation und Verwaltung erheblich verbessern. Die Entwicklung von Big Data schafft zwar enormen Wohlstand für Unternehmen, stellt jedoch auch eine ernsthafte Bedrohung für die Datensicherheit und den Schutz der Privatsphäre dar. Gleichzeitig können Daten „ohne Verlust verwendet“ werden, sodass sie oberflächlich nicht knapp erscheinen. Aufgrund der in Daten verborgenen wirtschaftlichen Vorteile werden sie jedoch von Unternehmen in „Datensätzen“ gesammelt und gespeichert, die mit speziellen technischen Maßnahmen ausgestattet worden sind. Dadurch sind die Datenressourcen tatsächlich knapp geworden. Infolgedessen wird der Wettbewerb um Daten unter Unternehmen immer härter (Wen Yuheng 2019). Zum Beispiel konkurrieren SF Express und Cainiao um „Logistikdaten“, Sina Weibo und Maimai um „Microblog-Daten“ und Huawei und Tencent um „WeChat-Daten“. All dies unterstreicht die dringende Notwendigkeit, das Recht auf Daten im Geschäftsbereich gesetzlich festzulegen. „Unternehmensdaten sind abgeleitete Daten, die von Unternehmen auf Grundlage des enormen Einsatzes von Material, Personal und Finanzmitteln durch tiefgreifende Entwicklung und systematische Integration erstellt werden, nachdem die Beziehungen zwischen den massiven und komplexen Originaldaten mithilfe von Tools für künstliche Intelligenz, mathematischen und statistischen analytischen Techniken und Data Mining-Technologien modelliert und hergestellt werden“ (Li Xiaoyu 2019). Unternehmensdaten umfassen nicht nur Daten, die die Grundsituation eines Unternehmens widerspiegeln,

wie Finanzdaten, Betriebsdaten (F & E, Beschaffung, Produktion, Vertrieb usw.) und Personalressourcendaten, aber auch personenbezogene Datensätze, die das Unternehmen direkt oder indirekt durch vertragliche Genehmigung sammelt (Shi Dan 2018). Die Unternehmensdaten enthalten einen enormen Gebrauchswert und Nutzungswert, sie können jedoch nicht uneingeschränkt verwendet werden. Wenn Unternehmen beispielsweise Daten erfassen, müssen sie den Zweck, die Methode und den Umfang der Datenerfassung und -nutzung klar angeben und die Zustimmung ihrer Kunden einholen. Wenn ein Unternehmen Daten verwendet, soll es den Umfang der Kundenautorisation nicht überschreiten oder über den bei der Datenerfassung angegebenen eigentlichen Zweck und Anwendung hinausgehen. Darüber hinaus darf es die Freiheit der Datennutzung, die öffentliche Sicherheit und die öffentlichen Interessen nicht beeinträchtigen.

2. Kompetenzkonfiguration von Unternehmensdaten

Die persönlichen rechtlichen Interessen von Unternehmensdaten können aus zwei Perspektiven verstanden werden. Einerseits in Bezug auf Datenerfassung stammt ein erheblicher Teil der von Unternehmen erhaltenen Daten aus den Datensubjekten. Andererseits in Bezug auf Datenzirkulation und Datennutzung sind Unternehmen nicht nur Datensammler, sondern auch Verarbeitende und Benutzer. Unternehmensdaten werden als Vermögenswerte oder Waren betrachtet, und das ist ein wichtiges Kennzeichen für Unternehmensdaten. Es ist nun zum normalen Zustand geworden, dass Unternehmen Daten sammeln, speichern, analysieren und verkaufen. Die groß angelegte Datenerfassung und -verarbeitung ist ein Teil der zentralen Wettbewerbsfähigkeit von Internetunternehmen geworden. Diese Unternehmen nehmen diese gesammelten Daten häufig als Kernbestandteil ihres Vermögens. Deshalb betonen Unternehmen die Freiheit der Datennutzung und die Tatsache, dass die von ihnen gesammelten und sortierten Daten ohne deren Zustimmung nicht von anderen verwendet werden dürfen. „Als Datensubjekt beanspruchen Unternehmen das absolute Eigentumsrecht auf Daten, die für ihre Produktion und

ihren Betrieb relevant sind, sowie das Vermögensrecht auf Daten, die sie gesammelt und sortiert haben“.¹⁰

Einige Wissenschaftler sind der Meinung, dass wir, wenn Daten zu Vermögen werden, basierend auf den Bedürfnissen des Datenbetriebs und angetrieben von Interessen, das Recht der Datenunternehmen auf Datenbetrieb und Dateneigentum anerkennen sollen. In gewissem Sinne hat das Datenbetriebsrecht unter anderem das wesentliche Merkmal des Monopolverchts. Es gilt nur speziell für bestimmte Angelegenheiten und hat seine Ausschließlichkeit, die durch gesetzliche Genehmigung oder behördliche Lizenzierung festgelegt wird. Das Recht auf Datenvermögen ist aber eine Art von absoluter Rechtszuerkennung, die gesetzlich für die Interessen vorgesehen sind, die die Datenbetreiber durch ihr Datenvermögensmanagement erhalten haben (Long Weiqiu 2017). „Die Dateninteressen von Unternehmen sind jedoch im Wesentlichen eine Art von verfügungsartigem Kontrollrecht. Die vom Kontrollrecht auf Unternehmensdaten aufgewiesene exklusive Wirksamkeit ist schwächer als das Eigentumsrecht, aber stärker als das Verfügungsrecht des relativen Rechts“ (Li Xiaoyu 2019). Das Kontrollrecht auf Unternehmensdaten besitzt positive und negative Befugnisse. Die positive Kompetenz verkörpert sich darin, dass Unternehmen als Rechtsinhaber berechtigt ist, ihre eigenen Daten direkt zu verarbeiten, zu sammeln, zu verwenden und zu handeln, ohne dass andere Parteien darin einmischen müssen. Die negative Funktionalität ermöglicht es Unternehmen, andere Parteien auszuschließen und sich vor unpassenden Eingriffen zu schützen, was Auswirkungen auf die Welt darstellt.

Bei Streitigkeiten im Zusammenhang mit Datenrechten gibt es Gerichtsurteile, die zwischen Rechten und Interessen unterscheiden. Zum Beispiel behauptete Taobao in Anklage von Taobao gegen Meijing in Bezug

10 Das Eigentumsrecht für Unternehmensdaten ist das Recht von Unternehmen, relevante Daten zu kontrollieren, zu verfügen und zu nutzen, einschließlich des Rechts auf Kontrolle, auf Vergütung, auf Änderung, auf Integrität und des Rechts auf gerichtliche Erleichterung usw. Siehe Wang Yuan, Huang Daoli & Yang Songru: „Forschung über die Natur und das Eigentum an Datenrechten.“ *Wissenschaftliche Managementforschung*, 2017, 5. Ausgabe.

auf einige Big-Data-Produkte,¹¹ dass Taobao direkt über das Dateneigentumsrecht auf die „mit bestimmten Algorithmen, anonymer Desensibilisierung, Filterung, Verfeinerung und Integrierung gebildeten abgeleitete Daten verfügte, während Meijing die mit technologischen Mitteln entwickelte Software und Plattform namens „Gugu Mutual Aid Platform“ benutzte und die abgeleitete Daten von Taobao erlangte und diese für ihre kommerziellen Zwecke verwendete. Taobao war der Ansicht, dass das Verhalten von Meijing einen unlauteren Wettbewerb darstellte und sein Dateneigentumsrecht verletzt hätte. Einerseits räumte das Gericht ein, dass Taobao über wettbewerbsfähige Eigentumsrechte und -interessen auf die aus ursprünglichen Daten „mit anonymer Desensibilisierung, Filterung, Verfeinerung und Integrierung gebildeten abgeleitete Daten verfügte; andererseits verweigerte es Taobao das Eigentumsrecht an primären Daten und abgeleitete Daten. Das Gericht gab jedoch keine direkte Antwort auf die Frage, was die wettbewerbsfähigen Eigentumsrechte und -interessen auf die abgeleiteten Daten des Unternehmens bedeuteten.

3. Neue Möglichkeiten zum Schutz der Rechte an Unternehmensdaten

Die vorhandenen Gerichtsentscheidungen befassen sich hauptsächlich mit dem Schutz von Unternehmensdaten nach den Bestimmungen des „Gesetzes zur Bekämpfung des unlauteren Wettbewerbs“. Der Schutz von Unternehmensdaten stellt jedoch ein neues Thema dar, das von unabhängiger Bedeutung ist. Dazu sollte neues Gesetz rechtzeitig erstellt werden. „Aus privatrechtlicher Sicht ist es unvermeidlich, dass wir in Bezug auf den Schutz von Unternehmensdaten von der Anwendung traditioneller Gesetze zu einem neuen Mechanismus für gesetzliche Legalisierung des Dateneigentumsrechts übergehen. Das ist sowohl zeitlich als auch sachlich zwangsläufig“ (Long Weiqiu 2018). Einige Wissenschaftler glauben jedoch, dass „die Rechte und Interessen an Unternehmensdaten in Bezug auf Rechtsattribut weder dingliche Rechte noch lediglich reine Rechte an geistigem Eigentum oder eigentümliche Rechte sind. Es ist ein

11 Siehe Hangzhou Railway Transportation Court (2017) Zhe 8601 Zivilurteil Nr. 4034.

Rechtsbündel von verschiedenen Rechten und Interessen, einschließlich zwei Typen wie legalisierte Rechte und gesetzlich geschützte Interessen“ (Li Yang & Li Xiaoyu 2019). Vor dem Hintergrund der neuen Technologien der Ära von Big Data müssen die Gesetze in Bezug auf Unternehmensdaten und -informationen ihren Schwerpunkt von der reinen Aufmerksamkeit auf Kontrollierbarkeit der Daten auf ein Gleichgewicht, d.h. Aufmerksamkeit sowohl auf Kontrollierbarkeit der Daten, als auch noch mehr auf angemessenen Datenfluss und Datennutzung und Verhinderung von Datenmissbrauch verlagern. Es liegt auf der Hand, dass die traditionellen strafrechtlichen Vorschriften, die lediglich aus der Perspektive von Geheimnissen (einschließlich Staatsgeheimnissen und Geschäftsgeheimnissen) oder Rechten des geistigen Eigentums geschaffen worden sind, möglicherweise erweitert werden muss (Tang Jiyao 2019). Daher ist eine rationale Übergangsform ratsam, den rechtlichen Schutz von Unternehmensdaten unter dem Gesichtspunkt des gesetzlichen Interessenschutzes, d.h. unter dem Gesichtspunkt neuer Arten von Rechten, zu untersuchen, bevor vorhandene Unternehmensdaten nicht durch gesetzliche Legalisierung der Rechte geschützt werden können. Einige Wissenschaftler schlagen auch vor, dass „Unternehmensdateninteressen geschützt werden sollten, indem das Kontrollrecht für Unternehmensdaten als eine neue Art von Rechten betrachtet wird“ (Li Xiaoyu 2019). Für Unternehmensdaten können nicht auf der Basis des dinglichen Besitzes sondern in gesetzlicher Form den Unternehmen „ausschließliche Rechte an Daten“ gewährt werden, damit Unternehmen die Existenz ihrer Rechte zeigen können. In Bezug auf die Wirksamkeit des Besitzes können Unternehmen aufgrund der Einschränkungen der Rechte der persönlichen Daten die von ihnen gesammelten und besitzenden Daten nicht vollständig kontrollieren, weil Einzelpersonen das Recht haben, ihre Daten zu löschen, zu korrigieren und zurückzunehmen usw. In Bezug auf Rechtssystem und Normen ist es notwendig, die Unternehmensdatenrechte einzuschränken und zu regeln, insbesondere müssen die Handlungen relevanter Unternehmen wie Erhebung, Verarbeitung und Nutzung von Daten gesetzlich reguliert werden. In der Praxis ändern und entwickeln sich sowohl die Anwendung von Datentechnologien als auch die Wettbewerbsmittel im Cyberspace ständig. Die entsprechende

Interessenverteilung zwischen Datenbetreibern, Internetnutzern und der Öffentlichkeit befindet sich ebenfalls in einem dynamischen Prozess des Gleichgewichts und des Ausgleichs.

(III) Rechte an Regierungsdaten

1. Regierungsdaten

Daten sind ein wichtiges Vermögen der Regierung. Sie sind ein wichtiges Mittel der Regierungsverwaltung und noch mehr eine Darstellung des Erfolges, den die Regierungsverwaltung erzielt hat. Sie sind eine Agglomeration von Daten aus Blöcken mit internen Zusammenhängen, die auf ein breites Spektrum öffentlicher Bedürfnisse und öffentlicher Anliegen vorausdeuten und großen Wert und Potenzial beinhalten. Diese Daten ändern grundlegend die Idee, das Paradigma, den Inhalt und Mittel der Regierungsverwaltung, transformieren das traditionelle Verwaltungsmodell, bei dem die Autorität durch Informationskontrolle und -monopol aufrechterhalten wird, und etablieren wirklich einen ganz neuen Mechanismus wie „mit Daten überzeugen, Entscheidung mittels Daten treffen, mittels Daten verwalten und mittels Daten bahnbrechen“, um damit den Aufbau einer digitalen Regierung zu fördern.

Im Allgemeinen umfassen Regierungsdaten alle Arten von Datenressourcen, die von den Volksregierungen und ihnen angeschlossenen Verwaltungsinstitutionen bei der gesetzmäßigen Erfüllung ihrer Aufgaben erstellt, beschafft, in einem bestimmten Format aufgezeichnet und gespeichert werden (Shi Dan 2018). Insbesondere verfügt jede Abteilung der Regierung über eine enorme Anzahl von Rohdaten, die das Fundament unserer Gesellschaft bilden, einschließlich meteorologischer Daten, Straßenverkehrsdaten, Stromdaten, Gerichtsdaten, Zolldaten, Ein- und Ausreisedaten und so weiter. Bei Regierungsdaten handelt es sich nur um ein Teil der massiven Big-Data-Ressourcen. Es bezieht sich insbesondere auf die Big Data, die die Regierungsstellen im Laufe der Jahre bei der Datenerfassung, dem Aufbau von IT-Systemen und der Abwicklung aller Arten von Geschäftsdiensten gesammelt haben. Die Regierungsdaten stehen

in engem Zusammenhang mit der Volkswirtschaft und dem Leben der Bevölkerung. Wenn dieser Teil der Daten effektiv zur Anwendung kommt, können Datenbenutzer mittels der Regierungsdaten innovative Anwendungen entwickeln, bessere Dienste bereitstellen, mehr Wert schaffen, das Wirtschaftswachstum fördern und die Transformation des Wirtschaftswachstumsmodells insgesamt erleichtern.

Auf der vierten Plenartagung des 19. Parteitag des Zentralkomitees der KP Chinas wurde vorgeschlagen, „Systeme und Regeln einzurichten und zu verbessern, damit die Verwaltung unter Anwendung von technologischen Mittel wie das Internet, Big Data, künstliche Intelligenz usw. besser geführt wird. Der Aufbau einer digitalen Regierung wird gefördert, eine ordnungsgemäße Datenteilhabe wird gestärkt und persönliche Informationen werden gesetzmäßig geschützt“. Anders als persönliche Daten und Unternehmensdaten sollten Regierungsdaten Merkmale von öffentlichen Gütern beibehalten, da die Regierung eher Inhaber öffentlicher Macht als Marktteilnehmer ist. Man soll sagen, dass Regierungsdaten alle von der gesamten Öffentlichkeit teilgehabt, als offene Daten behandelt und Datenfachleuten für Entwicklung und Nutzung zur Verfügung gestellt werden sollen mit der Ausnahme solcher Daten, die gemäß den einschlägigen Gesetzen und Vorschriften geheim gehalten werden sollen. Gegenwärtig baut der Staatsrat der Volksrepublik China ein nationales integriertes Big-Data-Center auf, um die technologische Integration, Geschäftsintegration und Datenintegration zu fördern und ein ebenen-, regions-, system-, abteilungs- und geschäftsübergreifendes synergetisches Management und Service zu realisieren. Die lokalen Regierungen arbeiten auch daran, Regierungsdaten für Teilhabe zu bündeln und viele von ihnen haben ihre Unterstützung für den Kauf von Daten aus der Gesellschaft ausdrücklich zum Ausdruck gebracht.

2. Aufbau des Regierungsdatenrechtssystems

Die Regierung ist diejenige, die Regierungsdaten verwaltet oder in gewissem Maße sogar die erste, die diese Daten erhält. Hier ist die Regierung das wichtigste Subjekt der Regierungsdaten. Regierungsdaten können nicht nur den Verwaltungsinstitutionen die Grundlage für wissenschaftliche

Entscheidungen bieten, sondern auch die Eigenschaft der Ressource haben, die wiederholt kopiert, verbreitet und genutzt werden können. Im Gegensatz zu dem abstrakten Konzept von „Daten“, das schwer zu definieren ist, können „Regierungsdaten“ wegen ihrer Besonderheit als Datensubjekt ihren Umfang reduzieren und unterschiedliche Rechteeigenschaft je nach der Teilhabe an verschiedenen Orten und unter verschiedenen Umständen ableiten. Dass die Regierungsdaten für Teilhabe offen sind, ist eine wichtige Grundlage für die Entwicklung von Big Data und wird zu einem allgemeinen Trend unserer Zeit. Die Offenheit und Teilhabe der Regierungsdaten sollen jedoch gemäß den gesetzlichen Bestimmungen erfolgen.

Wenn Verwaltungsinstitutionen Anbieter von Regierungsdaten sind, ist zumindest eines sicher: Diese Institutionen haben in gewissem Maße das Recht auf Kontrolle über die von ihnen bereitgestellten Daten, das heißt das Eigentumsrecht und Nutzungsrecht. Einerseits haben Verwaltungsinstitutionen als Benutzer von Regierungsdaten das Recht, die ihnen zur Verfügung stehenden Daten vollständig zu entwickeln und zu nutzen. Andererseits haben sie das Recht, die von anderen Regierungsabteilungen bereitgestellten Regierungsdaten „mit zusätzlichen Einschränkungen“ zu verwenden. Unter diesen „zusätzlichen Einschränkungen“ werden vor allem Einschränkungen verstanden, die sich auf Verarbeitung, Verwendung, Übertragung und Teilhabe von Regierungsdaten, die dieser Abteilung nicht gehören, beziehen: Erstens ist diese Einschränkung nur auf „Erfüllung von Verwaltungsaufgaben“, während Handlungen wie „Datentransaktionen und Datenaustausch“ für „kommerzielle Interessen“ verboten werden sollen. Zweitens gilt diese Einschränkung nur für den Rahmen zwischen den Abteilungen, die diese Daten miteinander teilen, während Abteilungen, die nicht an der Datenteilhabe teilnehmen, nicht in den Bereich der teilhabenden Subjekte einbezogen werden sollen (Zhang Yanan 2019). Entsprechend den Besonderheiten der Teilhabe von Regierungsdaten können das „Eigentumsrecht“ und „Nutzungsrecht“, die auf Basis der bestehenden Theorie über dingliche Rechte derivieren, die Eigentumsfessel der Teilhabe an Regierungsdaten in gewissem Maße lockern.

Als eine neue Art von Datenrechten umfassen die Regierungsdatenrechte nicht nur das Eigentumsrecht und Nutzungsrecht, sondern gibt es

auch viele andere Rechte, die innerhalb dieser Kategorie erschlossen werden sollen. Einige Wissenschaftler haben vorgeschlagen, dass „die Regierung als Vertreter des Staats das Verwaltungsrecht auf Big Data ausübt, das als Recht auf Datenerfassung, Datenkontrolle, Recht auf Planung der Datenentwicklung und Nutzungslizenz angesehen wird“ (Lü Tingjun 2017). Zum Zwecke der staatlichen Sicherheit und der sozialen öffentlichen Interessen hat die Regierung das Recht, Daten aus den politischen, wirtschaftlichen, kulturellen, sozialen und ökologischen Bereichen usw. mit bestimmten technischen Mitteln zu erhalten. Diese Befugnis, Datenressourcen kostenlos oder gegen Entgelt zu erhalten, ist Teil der Verwaltungsbefugnis der Regierung, die dem Verwaltungsgesetz unterliegt.¹² Daher sollen wir angesichts der systematischen Reform des Rechtssystems mit der Big-Data-Ressourcen und -Technologie als Kern so bald wie möglich ein neues Rechtssystem einrichten, das auf pluralistischen Macht- und Rechtssystemen basiert und das Datenrechtssystem im Mittelpunkt steht.

3. Öffnung und Regulierung der Regierungsdaten

Obwohl es zurzeit noch kein abschließendes Urteil über Datenrechte in verschiedenen Ländern der Welt gibt, kann der Wert von Daten

12 Datenkontrollmacht ist die normalisierte Macht der Datenverwaltungsbefugnisse, die sich auf die Kontrolle und tägliche Verwaltung der erfassten Big Data durch die Regierung bezieht, einschließlich des Verwaltungs- und Kontrollverhaltens wie verfahrensmäßige Klassifizierung, Sortierung, Speicherung und Schutz etc. von Big Data. Die Planungsmacht für Datenentwicklung ist die Gesamtplanung der Regierung für Entwicklung von Big Data, einschließlich mehrerer Verwaltungsbefugnisse wie Formulierung von Big Data-Richtlinien, künftiger Entwicklungspläne und der Koordinierung von Big Data-Entwicklungsobjekten. Die Befugnis der Datenlizenzierung ist eine der Kernbefugnisse des Rechts für Datenmanagement der Regierung. Die lizenzierte Benutzung von Big Data hängt nicht nur mit der Staatsicherheit und den öffentlichen Interessen, sondern auch mit den Rechten von Unternehmen, sozialen Organisationen und Bürgern zusammen. Daher ist das lizenzierte Nutzungsrecht von Big Data zum Mittelpunkt der sozialen Aufmerksamkeit und zum Kerninhalt der Schaffung von Rechtssystemen geworden.

als Ressource niemals gelehnt werden. So ist die Teilhabe an Regierungsdaten deshalb praktisch machbar, weil die Teilhabesubjekte der Regierungsdaten, die innerhalb der Regierungsstellen zirkulieren, die Verwaltungsbehörden sind, während der Umfang der Teilhabe nur auf gesetzmäßige Erfüllung ihrer Pflichten und Verantwortungen beschränkt und die Teilhabeaktivität nur auf zwei Handlungen wie „Benutzung“ oder „Lieferung“ eingeschränkt wird (Zhang Yanan 2019). Regierungsdaten sind die massivste, wichtigste und zentralste Komponente der sozialen Datenressourcen und haben ein hohes Potenzial für Mehrwert. Aufgrund der mangelnden Bereitschaft oder Schwierigkeit der Regierung, der Gesellschaft Zugang zu ihren Daten zu bieten, kann eine große Menge hochwertiger Daten jedoch langfristig nicht effektiv genutzt werden. „Aus der Perspektive des Verhältnisses zwischen öffentlichen und privaten Rechten sind Rechte auf Daten ein Grundrecht der Bürger. Die Bürger haben das Recht, über die von der Regierung kontrollierten Daten informiert zu werden und die Regierung ist auch verpflichtet, Regierungsdaten mit den Bürgern gemeinsam zu teilen“ (Lü Tingjun 2017).

Öffnung der Regierungsdaten ist ein Teil der Datenöffnung. Das bedeutet, dass die Regierung die Daten, die sie generiert und gesammelt haben und gebührend besitzt, die nach Erteilung der Erlaubnis zum Wissensaustausch der Öffentlichkeit bekannt geben und erlauben kann, an diesen gemeinsam teilzuhaben, zu verbreiten und revidieren und sogar kommerziell zu nutzen (Chen Shanglong 2019). In den letzten Jahren haben viele Länder aktive Anstrengungen unternommen, um Richtlinien für Öffnung der Regierungsdaten zu formulieren, relevante Rechtssysteme schrittweise einzurichten und zu verbessern sowie Aktivitäten im Zusammenhang mit Öffnung der Regierungsdaten zu leiten und zu regulieren. Öffnung der Regierungsdaten ist eine objektive Anforderung der Öffentlichkeit im Zeitalter von Big Data, die ihre Nachfrage nach staatlichen Datenressourcen von der Nachfrage nach Wissen zur Nachfrage nach Nutzung steiget. Um die Datennutzung für die Wertschöpfung zu erleichtern, ist es jedoch erforderlich, das Verhältnis zwischen Regierungsstellen und Öffentlichkeit neu zu gestalten, das Eigentumsrecht und die Verteilung der Vorteile aus staatlichen Datenbeständen vollständig zu berücksichtigen und die Mechanismen im Zusammenhang mit dem Eigentumsrecht,

Benutzungsrecht und Verdienstrecht der Regierungsdaten etc. ständig zu verbessern, die Kostenkontrolle für die Datenverwaltung durch die Regierung zu stärken und die Nachhaltigkeit der Datenverwaltung umfassend zu berücksichtigen etc.

Vor dem Hintergrund der Fortschritte der nationalen Big-Data-Strategie soll ein solides Politik- und Regulierungssystem für Öffnung und Teilhabe der Regierungsdaten eingerichtet werden. Das „ganze Richtlinienensystem kann in Infrastrukturschicht, Datenregulierungsschicht und Regierungsverwaltungsschicht eingeteilt werden“ (Huang Ruhua, Wen Fangfang & Huang Wen 2018). Konkret gesagt soll weiter überlegt werden, wie die Frage der Ungleichheit der Rechte auf Datenentwicklung und -nutzung zwischen verschiedenen Interessengruppen wie Regierung, Unternehmen, Gesellschaft und Hackern gelöst wird und die Funktionen und Pflichten, Aktivitäten und Aufgaben verschiedener Subjekte klar definiert werden, um ein Gleichgewicht zwischen der Maximierung des wirtschaftlichen und sozialen Wertes der Regierungsdaten und der Maximierung des Wertes der persönlichen Daten zu erreichen (Xia Yikun 2018). Gleichzeitig sollen wir aus globaler Sicht den gesamtplanmäßigen Aufbau und das Top-Level-Design der Regulierung von Regierungsdaten stärken, ein überregionales, abteilungsübergreifendes und systemübergreifendes offenes Datenteilhabesystem einrichten, um ein neues Muster der Datenregulierung mit pluralistischen Interaktionen zwischen Regierung und Gesellschaft zustande zu bringen. Dabei soll nicht nur das Eigentumsrecht der Regierungsdaten betont, sondern auch Wert auf Umgestaltung und Ausgrabung des Wertsystems der Regierungsdaten gelegt und Wege zu einer guten Datenverwaltung aus theoretischer, systematischer und methodischer Sicht gefunden werden.

Abschnitt III Konfrontation im Rahmen der Datenrechte

Im Zeitalter von Big Data haben sich sowohl die Konnotation als auch die Epitaxie von Recht und Macht dramatisch geändert. Private Datenrechte und öffentliche Datenmacht befinden sich im Cyberspace normalerweise

in einem Zustand der gegenseitigen Konfrontation, des gegenseitigen Wettbewerbs und des wechselseitigen Kontrollgleichgewichts. In Bezug auf entsprechende Datenrechtsaufteilung haben Einzelpersonen und Unternehmen aufgrund der Überlegung der eigenen Interessen Rechtsansprüche unterschiedlicher Art geltend gemacht, was im tief gehenden Sinne Wettbewerb um Interessen zwischen persönlichen Datenrechten und -interessen und der Datennutzung von Unternehmen, zwischen Einzelpersonen und Regierung sowie zwischen verschiedenen Unternehmen darstellt. Die Übertragung von Datenrechten und der Rückgang der Datenmacht sind unvermeidlicher Trend der Entwicklung von Datenrechten und auch zwangsläufige Anforderungen aufgrund der Unterschiede der Einzelpersonen und der gruppenweisen Teilhabe. Deshalb kann der Wert von Big Data möglicherweise nur dann optimal abgegeben werden, wenn das bestehende stabile Rechtssystem durchgebrochen und angepasst wird und die Datenrechte und -interessen von Einzelpersonen, Unternehmen und der Regierung ausgeglichen und koordiniert werden, nachdem die Liste der datenbezogenen Rechte erweitert und verfeinert wird.

(I) Übertragung privater Datenrechte

1. Datenrechte und private Rechte

Personenbezogene Daten stammen aus persönlichen Verhalten, sodass diese Rechte der Person gehören, die diese Daten bereitstellt und besitzt. Der persönliche Besitz ist die vorausgesetzte Bedingung und der richtige Grund für die Entstehung des Systems der Privatrechte. Die sogenannten Privatrechte, also private Rechte, sind eine Art von persönlichen Rechten, privateigenen Rechten und Rechten der Privatinteressen. Ein Teil der Daten ist ausschließlich im Besitz einer Person, d.h., dass sie die Eigenschaft der Privatrechte besitzt. Das Merkmal von Daten bestimmt, dass das Attribut der Privatrechte pluralistische Eigenschaften hat, die sich hauptsächlich in Eigenschaft der Persönlichkeit und des Eigentums darstellen. Datenrechte sind eine Kombination aus Persönlichkeitsrechten

und Eigentumsrechten. Diese beiden Arten von Rechtsattribut existieren nebeneinander und sind untrennbar miteinander verbunden, sodass sie die Grenzen der traditionellen Bürgerrechte durchbrochen haben und zu einer neuen Art von Bürgerrechten geworden sind. Deshalb können sie nicht mit den traditionellen zivilrechtlichen Bestimmungen zu verordnen. Daher ist es dringend nötig und unausbleiblich, ein neues Rechtssystem einzurichten. Beide Interessenmerkmale der Datenpersönlichkeitsrechte und Datenvermögensrechte haben alle einen wirtschaftlichen Wert. So zielt unsere Analyse der Eigenschaft der Privatrechte hier vor allem darauf ab, herauszufinden, welches Schutzmodell für Datenrechte besser ist, entweder das Schutzmodell der Persönlichkeitsrechte oder das der Vermögensrechte.

2. Verbreitung von Datenrechten

Obwohl Datenrechte erst im Zeitalter von Big Data vorgestellt worden sind, besteht diese Idee jedoch schon lange. Daten im traditionellen Sinne wie persönliche Informationen, Privatsphäre, Wissensgesetzmäßigkeit und Handelsgeheimnisse usw. wurden in vielen Ländern in den Geltungsbereich der zivilen Rechte aufgenommen. Der Vorschlag zu Datenrechten bedeutet sowohl Entwicklung der traditionellen zivilen Rechte als auch den Aufbau einer neuen Art von Rechten. Dies liegt darin, dass der Umfang von Objekten der Datenrechte jetzt schon zu einer allgemeingültigen Datenebene erweitert wurde. Er umfasst nicht nur eindeutige persönliche Informationen und Wissensregeln, sondern auch unzählige andere Arten von Daten, die dem Schein nach nicht zusammenhängend sind. Die Nutzung und Erforschung solcher Daten mit relevanten Technologien ist das Kernwesen des Big-Data-Zeitalters. Die sich daraus ergebenden Rechte gehen schon über den Rahmen der traditionellen zivilen Rechte hinaus. Mit zunehmendem Bewusstsein und zunehmender Sorge um den Datenschutz wachsen Datenrechte rasch heran. Im Gegensatz zur Entwicklung privater Rechte in der Vergangenheit erfolgt die Entwicklung von Datenrechten jedoch eindeutig in Form von Ausbreitung. Vor allem ist die Ausbreitung von Objekten der Datenrechte sichtbar. Zu den Objekten der Datenrechte gehörten früher nur einige Teilobjekte wie

Kenntnisse, Geheimnisse und Privatsphäre usw., während diese Daten auch von traditionellen elektronischen Daten zu Daten in aller Form ausgebreitet sind, sodass die Datenrechte allgegenwärtig sind. Zweitens tritt Ausbreitung von Subjekten der Datenrechte auf, wobei es sich um Doppelausbreitung in Form von Menge und Typ handelt. In Bezug auf Typ weiten die Subjekte der Datenrechte von allgemeinen juristischen Personen zu juristischen oder nichtjuristischen Organisationen wie Körperschaft, Unternehmen und Regierung usw. aus, während sie mengenmäßig derart erscheinen, dass alle Dateninhaber sicher gewisse Ansprüche auf Datenrechte erheben. Mit weiteren Fortschritten auf dem Gebiet der Big Data werden immer mehr Subjekte ihre Ansprüche auf Datenrechte behaupten. Zum Schluss erfolgt die Ausbreitung der Nutzung der Datenrechte. Mit dem raschen Wachstum des gesamten Datenvolumens und der Klärung seines Status als eine Art Ressource wird der Raum für die Ausübung ihrer Datenrechte immer größer und die Anwendungshäufigkeit auch immer höher. Die Ausübung der Datenrechte wird durch offensichtliche Ausbreitung gekennzeichnet.

3. Teilhabe an Datenrechten

Einzelpersonen sind Produzenten von Daten. Die Regierung ist die größte Besitzerin der Daten, während Unternehmen die Hauptkraft sind, die die Entwicklung und Anwendung von Daten fördern. Angetrieben von Dateninteressen setzen Unternehmen große Mengen an Kapital und Personalressourcen ein, um Datentechnologie ständig zu entwickeln und zu verbessern, neue Methoden für die Datenproduktion, -erfassung und -analyse kontinuierlich zu innovieren, Vervollständigungen bei verschiedenen Datenaktivitäten stets anzustreben und verschiedene Datenbeziehungen in Ordnung zu bringen und damit Datenboom und hohe Wirtschaftlichkeit zu erreichen. Vom traditionellen Informationsschutz bis zu „Allgemeinen Datenschutzverordnung“ ist der Schutz der privaten Datenrechte von schwach zu stark geworden. Ein solcher Schutz, ob er schwach oder stark ist, ist jedoch für die Entwicklung von Big Data nicht günstig und könnte zu Ungleichgewicht bei der Verteilung von Datenrechten führen. Um ein Gleichgewicht der Datenrechte zu erreichen, ist

es besonders wichtig, neben der Einschränkung der öffentlichen Datenmacht eine angemessene Übertragung privater Datenrechte sicherzustellen. Wenn personenbezogene Daten undifferenziert äußerst streng geschützt werden, könnte dies zwei nachteilige Folgen haben: Zum einen hängt die Entwicklung von Big Data stark von einer guten Gesamtdatenumgebung ab, während ein reibungsloser und regsamer Datenverkehr einen wichtigen Grundstein für den Aufbau einer guten Datenumgebung bildet. Unter diesem Schutzmodell wird der Datenverkehr jedoch ernsthaft behindert und die Entwicklung von Big Data in hohem Maße kraftlos und sogar gestört. Zum Beispiel hat die „Allgemeine Datenschutzverordnung“ als „strengstes Datenschutzgesetz in der Geschichte“ ein enormes GDP-Verlustrisiko verursacht.¹³ Andererseits enthält Big Data auch großen Wert. Angesichts großer Interessen erhöht ein zu strenger Schutz das Risiko datenbezogener Straftaten, wodurch der Schutz personenbezogener Daten in einem Teufelskreis gerät, in dem je strenger der Schutz ist, ist das Risiko desto größer, während eine lockerere Kontrolle Chaos mit sich bringt.

Die Daten zeigen typische Merkmale wie Nichtausschließbarkeit, Nichtverbrauchbarkeit und Reproduzierbarkeit usw. Sie sollen aus Schutzgründen nicht in eine seltene Ressource verwandelt werden. Stattdessen sollen sie als universelle, allgemeine, bequeme und erneuerbare „wiederverwendbare Ressourcen“ bleiben.¹⁴ Das Wesentliche der Übertragung privater Datenrechte besteht darin, Hindernisse für den Datenfluss so weit wie möglich zu beseitigen, einen reibungslosen Datenverkehr zu fördern

13 Die Datenschutzgrundverordnung ist für Schutz personenbezogener Daten sehr streng. Für die Technologie- und Finanzindustrie wird die Umsetzung der Verordnung Schwierigkeiten des persönlichen Zugangs zu Krediten weiter verschärfen. Nach Schätzungen von Deloitte Touche Tohmatsu Limited wird die Verordnung den Konsumkredit in der EU um 19 Prozent senken und zu einem jährlichen Verlust des GDP von 83 Milliarden Euro und einer Arbeitslosigkeit von 1,4 Millionen Menschen führen.

14 Nutzererneuerbare Ressourcen beziehen sich auf diejenigen Ressourcen, die durch Verwendung nicht verbraucht, sondern dadurch wieder vermehrt werden können. Beispiele sind Daten, Technologie und Wissen usw.

und so den Wert der Daten maximal auszulösen. Die Teilhabe befindet sich im Mittelbereich zwischen Übertragung und Einschränkung. Die Datenteilhabe ist ein grundlegendes Wertkonzept im Zeitalter von Big Data. Die gemeinsame Nutzung von Datenrechten ist nicht nur ein Anspruch der Datenentwicklung an sich, sondern auch ein wichtiger Weg, Datenrechte von einem Ungleichgewicht zu einem Gleichgewicht zu bringen.

In Anbetracht dessen, dass Daten eine typische „wiederverwendbare Ressource“ sind, ist die maximale Nutzung ihre wesentliche Anforderung, und die Teilhabe ist der beste Weg, um diese Anforderung zu erfüllen. Aus Sicht des Rechts sind Teilhabe und Besitz der wesentliche Unterschied zwischen Datenrechten und dinglichen Rechten. Der Grund dafür liegt darin, dass die Interessen des Rechtssubjekts der Dinge durch Existenz des Besitzrechts während der Übergabe des Nutzungsrechts der Dinge nicht beeinträchtigt werden können, weil die Rechtssubjekte immer noch über Kontrollrecht diese Dinge verfügen. Ganz anders ist es aber bei Datenrechten, wird die Partei, die das Recht zur Nutzung erhält, die Daten vollständig besitzt, sobald das Recht zur Nutzung der Daten übergeben worden ist und die Daten geraten außer Kontrolle der primären Rechtsinhaber. Zu diesem Zeitpunkt ist das Besitzrecht auf diese Daten bedeutungslos. Datenrechte haben die Beschränkungen von „ein Recht für ein Ding“ und „Dinge müssen greifbar sein“ durchgebrochen. Dies äußert sich häufig darin, dass ein Datum mehrere Rechte hat. Für Daten ist die Betonung des Datenteilhaberechts so wichtig wie die Betonung des Besitzrechts des Sachenrechts. Das ist ein zwangsläufiger Übergang von der bestmöglichen Nutzung von Dingen zur bestmöglichen Nutzung von Daten (Schlüssel-Labor für Big Data Strategie 2019, S. 266).

(II) Einschränkungen der öffentlichen Datenmächte

1. Datenrechte als öffentliche Datenmacht

Datenmacht hat in der Natur Attribut der öffentlichen Macht. In Bezug auf die Folgeorientierung, die sich aus der Datenmacht ergeben wird, dient die virtuelle Cyberspace-Welt als Spiegelwelt der realen Welt, damit

die öffentliche Macht neuen Trägerraum und neue Realisierungswege erhält, während die Öffentlichkeit die damit verbundene Bequemlichkeit durch den Cyberspace und relevante Technologien genießt, kann sie gleichzeitig die Sorge vor böswilligen Angriffen, Angst vor Mitreißen der dunklen Macht und keinerlei Flucht in der Cyberwelt abwerfen. Die hohe Integration von Cyberspace und der physischen Welt hat ein Muster gegenseitiger Unabhängigkeit und gegenseitiger Beeinflussung zwischen ihnen gebildet. Das Ergebnis der Ausübung von Datenmacht kann sich auf die gesetzlich geschützten öffentlichen Interessen auswirken. Aus wirtschaftlicher Sicht kann Big Data eine Art „quasi öffentliche Güter“ darstellen, die sowohl „öffentlicher als auch privater Natur“ des Gesetzes sind. Dem Wesen nach ist es in erster Linie eine Art privates Recht, aber in Bezug auf Ergebnis und Auswirkung der Ausübung von Datenmacht kann sie die öffentlichen Interessen beeinflussen und so hat sie auch die Merkmale der öffentlichen Macht. Als eine Art privater Rechte müssen Datenrechte gesetzlich geregelt werden. Einzelpersonen dürfen keine „Daten monopolisieren“ oder keine öffentlichen Interessen opfern, um personenbezogene Daten zu schützen. Gäbe es kein Gegengewicht von öffentlichen Interessen, würde das Jagen nach privaten Interessen die Gesellschaft auch dazu verleiten und das Dateneigentumsrechtssystem würde stattdessen ein Fesseln für die Entwicklung der Big-Data-Industrie. In Chinas sozialistischem Rechtssystem werden sowohl öffentliche als auch private Rechte gesetzlich geregelt und geschützt. Der Schutz der Rechte der persönlichen Daten ist nur einer unserer Zwecke. Was noch wichtiger ist, ist der Schutz der öffentlichen Interessen und die Maximierung des Werts von Daten.¹⁵ „Der Vorschlag für Rechte auf

15 Professor Xue Zhaofeng, ein Ökonom, geht bei der Analyse der schrittweisen Erfolge im Buch „Internet Economic Governance Manual“ davon aus, dass sich die Governance-Regeln in Richtung eines Gleichgewichtspunkts bewegen können, der die Maximierung des Werts von Datenbeständen darstellt. Wer die Daten gut nutzen kann, ihm könnten diese Daten möglicherweise gehören. Die Governance-Regeln, mit denen der potenzielle Wert von Datenbeständen maximiert werden kann, und das Prinzip zur Definition von Eigentumsrechten, mit dem Datenbestände voll genutzt werden können, sind gute und stabile Regeln, die von allen einhalten wollen und gut überleben können.

Daten steht genau im Einklang mit Moralitätstheorie. Das heißt, dass Bürger ihre Datenrechte vor der Regierung beanspruchen, gilt als eine Art Rechtsbehelf, Vorsichtsmaßnahme oder negative Behauptung, ihr Hauptziel liegt darin, Bürger vor Verletzung ihrer privaten Rechte durch öffentliche Macht und andere enorme Datenkontrolleure zu schützen“ (Liu Jiangan 2016).

2. Expansion der Datenmacht

Die öffentliche Macht an sich ist von Natur aus obligatorisch und expansiv. Daher ist es notwendig, sie unter Kontrolle zu halten. Im Zeitalter von Big Data haben das Fehlen eines Datenrechtssystems und die Selbstexpansion der öffentlichen Macht zum Missbrauch der öffentlichen Macht der Daten geführt, was in unterschiedlichem Maße zu einer Verletzung der Rechte der persönlichen Daten geführt hat. Dies spiegelt sich hauptsächlich in den folgenden zwei Aspekten wider:

Erstens: private Nutzung öffentlicher Macht für eigene Interessen. Die vage Grenze zwischen den Rechten und der Macht der Subjekte der pluralistischen Regulierung ermöglicht es, dass öffentliche Macht und private Rechte bis zu einem gewissen Grad ineinander eindringen. Technisch gesehen können die Bürger die Freiheit genießen, ihre Rechte auf persönlichen Daten nur dann auszuüben, wenn sie der Kontrolle durch die öffentliche Datenmacht unterliegen. In der Realität wird öffentliche Datenmacht jedoch öfters für private Interessen genutzt, was die Sicherheit privater Datenrechte beeinträchtigt. Es gibt zwei Formen der privaten Nutzung öffentlicher Macht für eigene Interessen: Eine ist der Missbrauch der öffentlichen Datenmacht, was bedeutet, dass die Datennutzung gegen festgelegte Regeln und Verfahren verstößt und die Freiheit der Bürger für Nutzung ihrer privaten Rechte verletzt. Die andere ist das Suchen und Festlegen von Mietern auf einigen Plattformen, was auch die Rechte der Bürger auf persönlichen Daten verletzt.

Zweitens ist der Schwerpunkt der Macht geneigt. In der physischen Welt ist die öffentliche Macht den privaten Rechten immer überlegen. Öffentliche Macht, die von Natur aus sehr expansiv ist, neigt dazu, den

Raum der privaten Rechte zu komprimieren. Solcher Konflikt spielt sich im Cyberspace weiter ab. Subjekte der Datenmacht wandeln allmählich in Subjekte um, die in Bezug auf Ressourcen relative Überlegenheit besitzen, während diese meistens Big Data oder Big-Data-bezogene Ressourcen sind. Daten rekonstruieren den Wert der modernen Macht, wodurch sich der Kapitalgebrauch auch geändert hat. Die Anwendung der Datenmacht verändert die Position von Machtsubjekten auf dem Markt, beraubt die Subjektmacht von schwachen Inhabern der Big Data und bringt neue Subjekte der Kapitalmacht zustande. Gleichzeitig kann die Verstärkung der Datenmacht die Fähigkeit der Machtinhaber erhöhen, den Markt zu kontrollieren und zu monopolisieren (Tong Linjie & Guo Chengcheng 2019). Die Entwicklung der modernen Informationstechnologie hat die Informationsasymmetrie zwischen Regierung, Unternehmen und der Bevölkerung verschlimmert und das noch schwerere Gewicht auf diejenigen gelegt, die die öffentliche Macht in ihren Händen halten (Zheng Ge 2016).

Die Grenze zwischen öffentlicher Macht und privaten Rechten wird neu definiert, wobei der Raum privater Rechte gegen öffentliche Macht immer mehr verringert wird. Die Datenmacht ist absolut isoliert und von virtueller Natur, wobei es auch Datenrisiken und blinde Flecken bei der Ausübung der Macht gibt, die ganz möglicherweise zu einem schwarzen Loch der Ethik wie soziale Anomie und politische Unordnung im Umgang mit dem Interessenverhältnis zwischen verschiedenen Subjekten und Objekten führen könnten (Lin Qifu & He Jingchao 2016). Die angemessene Ausweitung der Datenmacht ist eine wichtige Voraussetzung für die rasche Entwicklung von Big Data im frühen Stadium, aber ihre uneingeschränkte Selbstexpansion wird unbedingt zu einer Verringerung oder Verletzung von Datenrechten führen. Nur wenn wir ein allgemeines Gleichgewicht zwischen Datenrechten und Datenmacht herstellen und aufrechterhalten, kann mehr Raum für gegenseitiges Vertrauen für die sprunghafte Entwicklung von Big Data gewonnen werden (He Dingding 2018).

3. Abnahme der Datenmacht

Datenmacht und Datenrechte sind Zwillinge. Im traditionellen Rechtsrahmen der Rechte gegen Macht wird die Selbstkontrolle über persönliche Daten eingesetzt, um den Missbrauch der Regierungsmacht und dadurch die Verletzung der Privatsphäre zu verhindern (Wang Xiuzhe 2018). Fast gleichzeitig mit dem rasanten Wachstum der Datenrechte beschleunigt sich auch die Bildung von Datenmacht: Einerseits vermehren sich Ansprüche an Datenrechte, die durch Entwicklung von Big Data mit sich gebracht worden sind, die fordern an, die Datenmacht als legitime Grundlage und praktische Garantie der Datenrechte aufzubauen, weil die Datenrechte ohne staatliche Macht niemals existieren können. Andererseits ist es für die Regierung das Prioritätsprinzip, die Entwicklung von Big Data als eine neue Sache unter ihrer Kontrolle sicherzustellen. Dazu soll die Nutzung von Datenmacht in einem bestimmten Maße eingeschränkt und standardisiert werden und die Nutzung von Datenrechten in einem angemessenen Bereich und auf eine rationale Weise halten.

Sollte die Datenmacht bei der Entwicklung von Big Data nicht reguliert werden, käme es zu Umständen wie Nichttätigkeiten, willkürlichen Tätigkeiten und übermäßigen Eingriffen. So würde die Implementierung von Datenmacht ernsthaft behindert und der Schutz von Datenrechten auch unmöglich sein, was sowohl für die Entwicklung von Big Data als auch für die soziale Stabilität insgesamt sehr schädlich ist. Nur durch die Regulierung der öffentlichen Datenmacht und Verhinderung des Missbrauchs der öffentlichen Datenmacht können die privaten Datenrechte wirksam geschützt werden. Die Regulierung der öffentlichen Datenmacht bedeutet jedoch nicht, die Autorität der öffentlichen Datenmacht abzuschwächen, sondern soll die Ausübung der öffentlichen Datenmacht aber mittels einschlägiger Regeln und Verfahren reguliert werden. So kann die Autorität der öffentlichen Datenmacht nicht nur nicht geschwächt werden, sondern kann sie noch besser in Funktion treten.

Auf lange Sicht ist die Expansion der Datenmacht unvermeidlich, ebenso wie ihr Rückgang. Der Wert von Daten liegt nicht in der großen Menge, sondern in der breiten Nutzung. Heute, da die Datenaktivitäten

schnell und regsam zunehmen, nimmt die Datenmacht obwohl ständig zu und expandiert sich sogar, wird sie sich an einem bestimmten Punkt unweigerlich drehen und verfallen. Dies liegt daran, dass eine starke Datenmacht als administrative und rechtliche Unterstützung in der frühen Phase der Big-Data-Entwicklung erforderlich ist, um in kurzer Zeit eine ausreichende Triebkraft für die Entwicklung von Big Data bereitzustellen. Mit der Reife der Big-Data-Branche ist das Vorhandensein einiger Art Datenmacht jedoch zu einem Hindernis für die weitere Entwicklung von Big Data geworden, wobei die Ansprüche auf Datenrechte erfordern auch Einräumung der Datenmacht, um mehr Raum für weitere Entwicklung zu schaffen. Dies führt zu einem Rückgang der Datenmacht. Diese Abnahme oder Niedergang ist jedoch kein Aussterben. Das ist eine Machtübergabe auf Basis der grundlegenden Prinzipien zur Sicherstellung der Datensicherheit wie staatlicher Sicherheit und Schutz der Privatsphäre etc. Diese Machtübertragung wird von der Eigenschaft des freien Datenverkehrs bestimmt. Sie ist die Grundlage, auf der das Beste aus Daten herausgeholt werden kann und spielt eine äußerst wichtige Rolle für die zukünftige Entwicklung unserer Gesellschaft.

(III) Die öffentliche Macht geht ins Reich des privaten Datenrechts

1. Die öffentliche Macht geht ins Reich des privaten Datenrechts

Es waren Juristen im alten Rom, die das Recht zunächst in öffentliches und privates Recht aufteilten. Ausgehend vom Ziel betrachtete Domitius Ulpianus¹⁶ das Gesetz zum Schutz nationaler Interessen und öffentlicher Interessen als öffentliches Recht und das Gesetz zum Schutz privater

16 Domitius Ulpianus schuf initiativ das System des „öffentlichen Rechts“ und des „Privatrechts“ in der Rechtsprechung und befürwortete das System des Schutzes des Privateigentums von Sklavenbesitzern, das erhebliche Auswirkungen auf die spätere kapitalistische Rechtskunde hat. Zu seinen repräsentativen Werken gehören Ad Edictum, Libri ad Sabinum und De omnibus tribunalibus.

Interessen als Privatrecht. Gegenwärtig stimmen die meisten Juristen in Ländern des kontinental-europäischen Rechtssystems der Theorie der Anpassung der Beziehungen zu, wonach „das Privatrecht das Gesetz ist, das die Beziehungen zwischen gleichberechtigten Subjekten im zivilen Leben regelt, während das öffentliche Recht das Gesetz ist, das die Beziehungen zwischen staatlichen Organen und Beziehungen zwischen dem Staat und seinen Bürgern im politischen Leben regelt. In diesem Sinne fällt auch das Gesetz zur Regelung der zivilrechtlichen Beziehungen zwischen dem Staat und seinen Bürgern in die Kategorie des Privatrechts. In China ist das Strafrecht und Verwaltungsrecht usw. das typischste öffentliche Recht, während das Zivilrecht in die Kategorie des Privatrechts fällt. Mit der Unterstützung von der Theorie der Beziehungsanpassung gibt es eine klare Grenze zwischen dem öffentlichen Recht und privatrecht“ (Chen Hongzhi 2018).

Der Auftritt des öffentlichen Rechts im Bereich des privaten Rechts bedeutet, dass die öffentliche Macht aus irgendeinem Bedürfnis im Bereich des privaten Rechts interveniert, das die Beziehungen zwischen gleichberechtigten Subjekten regeln, und dass die öffentliche Macht somit ins autonome Verhalten des privaten Rechts bis zu einem gewissen Grad eingreift (Wang Chunye 2008). Mit dem Fortschritt der Digitalisierung treten verschiedene soziale Widersprüche im Zusammenhang mit Rechten persönlicher Daten häufiger auf und sammeln stets an, und auch die Häufigkeit der Intervention von öffentlicher Macht nimmt kontinuierlich zu. Erstens aufgrund der bestehenden Datenlücke und des Datenmonopols und der Ungleichheit des Status der verschiedenen privatrechtlichen Subjekte usw. zieht das öffentliche Recht den eigentlich zum Bereich des privaten Rechts gehörenden Inhalt an sich, damit das öffentliche Recht gesetzmäßig darin einmischen kann und so die Verwirklichung des Eintritts des öffentlichen Rechts ins Reich des privaten Rechts ermöglichen kann, um die Rechte schutzbedürftiger Gruppen zu schützen und den Missbrauch der Monopolmacht durch wenige Mächtigen einzudämmen, wenn extreme Ungerechtigkeit von der Autonomie des privaten Rechts verursacht worden ist. Zweitens können private Datenrechte in die Kategorie der bürgerlichen privaten Rechte einbezogen werden, wenn die Verletzung privater Datenrechte die öffentlichen Interessen offensichtlich beeinträchtigt, da die privaten Datenrechte als eine Art Eigentumsrecht in

der Natur angesehen werden können. Private Rechte sind zivilrechtliche Rechte. Im Bereich der Rechtsbeziehungen der zivilrechtlichen Rechte haben alle Parteien gleiche Stellung, auch wenn die staatlichen Behörden eine Partei sind, soll der Wille der zivilen Subjekte im Umgang mit allem, was mit Bürgerrechten zu tun hat, einschließlich privater Datenrechte, uneingeschränkt respektiert werden.

Als eine neue Art von Übereinstimmung mit zivilrechtlichen Rechten soll sich das Ziel der Gesetzgebung zu diesen persönlichen Datenrechten mehr nach dem Schutz von Interessen, der Verteidigung gegen Verletzungen der Datenrechte durch andere Subjekte und der Möglichkeit neigen, dass Datenrechte im Bereich des Gesetzes direkt ihre rechtliche Rolle spielen können. Die Anerkennung von Datenrechten im Bereich des Privatrechts soll eng mit Rechtsbehelfen im Falle von Beschädigung verbunden sein, und Datenrechte sollen sowohl vom privatrechtlichen Bereich als auch vom Bereich des öffentlichen Rechts gemeinsam geschützt werden (Lü Zhixiang & Zhang Qiang 2019). Wenn die öffentliche Macht in Bereich der privaten Datenrechte interveniert, wird der Grundsatz der Autonomie im Privatrecht in gewissem Maße eingeschränkt, hat jedoch keinen Einfluss auf das Wesen des Zivilrechts und der privaten Rechte geübt. Die Intervention öffentlicher Macht in Bereich der privaten Datenrechte unterstreicht einerseits das Eingreifen des Staates ins Datenrechtssystem, andererseits betont sie Schaffung eines Ausgleichsmechanismus zwischen persönlichen Interessen der Schöpfer und öffentlichen Interessen der Gesellschaft. Dies wird die wesentliche Eigenschaft der Datenrechte aber auf keinen Fall ändern, sodass sich die privaten Rechte zu einer Mischung von privaten Rechten und öffentlicher Macht entwickelt.

2. Tendenz der Intervention der öffentlichen Macht in Bereich der privaten Datenrechte

In der heutigen Ära, da Faktor für das Eingreifen der öffentlichen Macht in den Schutz von Datenrechten zunimmt, beeinträchtigen verschiedene Arten von unerlaubten Handlungen nicht nur die Rechte von Datenrechtinhabern und dämpfen die Vitalität der Entwicklung von Unternehmen, sondern schädigen sie auch ernsthaft die öffentlichen Interessen der Gesellschaft. Der Schutz der Datenrechte soll auf Einzelpersonen basieren,

um verschiedene Rechte der Bürger auf personenbezogene Daten und ihre Verarbeitungsaktivitäten zu schützen. Die Bestimmungen zu Rechten persönlicher Daten könnten jedoch leicht virtualisiert werden, so ist es nicht ausreichend, bloß diese Rechte zu regeln. Außerdem führt die relativ große Differenz in der Datenverarbeitungskapazität zwischen verschiedenen Parteien in Bezug auf persönliche Daten zu einem Ungleichgewicht, wobei eine Partei enorme Vorteile im Wettbewerb genießt, und diese Wettbewerbsvorteile erleichtern einige Subjekte, Interessen zu erfassen, die eigentlich anderen Subjekten gehören sollten. Daher ist die Regierung mit ihrer öffentlichen Macht diejenige, die ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Entwicklung der Big-Data-Branche herstellen soll. Sie soll einerseits die Datensicherheit gewährleisten, andererseits die Datenvitalität anregen und die gesunde Entwicklung der Datenwirtschaft stets fördern, um es zu realisieren, dass die Daten wirklich von den Volksmassen zum Wohle der Bevölkerung verwendet werden.

„Angesichts der Bedrohung der Rechte personenbezogener Daten durch den Staat kann das Zivilrecht allein keinen ausreichenden Schutz bieten. Es ist dringendst notwendig, die öffentliche Macht auf der Grundlage der Grundsätze des rechtlichen Vorbehalts, des ordnungsgemäßen Verfahrens und der Verhältnismäßigkeit zu regeln“ (Zhang Xinbao 2018). Beispielsweise haben sowohl das „Passgesetz der Volksrepublik China“ als auch das „Gesetz der Volksrepublik China über gebietsansässige Personalausweise“ Bestimmungen über den Schutz gesammelter persönlicher Informationen vorgeschrieben. Bisher hat China noch kein spezielles Gesetz zum Schutz personenbezogener Daten eingeführt. Obwohl es mehr als 70 Gesetze und Vorschriften zum Schutz personenbezogener Daten gibt, leisten sie alle Abhilfe durch nachträgliche Bestrafung aber ohne vorherigen Schutz. In Bezug auf den mittelbaren Schutz persönlicher Daten werden sie im Allgemeinen durch den Schutz der mit persönlichen Daten im Zusammenhang stehenden Bereiche wie Privatsphäre und Menschlichkeitswürde etc. geschützt.

In diesem Zusammenhang ist die gegenseitige Durchdringung und Integration von öffentlichem und privatem Recht zu einem wichtigen Trend der Entwicklung des Datenrechtsschutzes geworden. Einerseits hat „das öffentliche Recht ständig in den Bereich der privaten Rechte eingedrungen, um die Unzulänglichkeit der Anpassung durch traditionelles Privatrecht auszugleichen, die aber zur Einmischung des öffentlichen Rechts in den Bereich der

privaten Rechte führt“ (Wang Chunye 2008). Auf der anderen Seite verfolgt der Staat den traditionellen Ansatz des öffentlichen Rechts und führt eine Vielzahl von privatrechtlichen Systemen und Begriffen als Beispiel ein und lernt daraus, um den Zweck des öffentlichen Rechts besser zu verwirklichen, wodurch sich das öffentliche Recht auch in den Bereich der privaten Rechte gedrängt hat. Im Allgemeinen sollen personenbezogene Daten als öffentliche Güter geregelt werden. Die Verwendung personenbezogener Daten soll von speziellen Regierungsbehörden als Subjekt geregelt werden. Das gesetzliche Wesen der Datenverwaltung an sich soll eher in den Bereich des öffentlichen Rechts als des Privatrechts fallen. Ziel der Datenverwaltung ist es dann, die freie Teilhabe an personenbezogenen Daten im Interesse der öffentlichen Interessen und der öffentlichen Sicherheit zu fördern (Wu Weiguang 2016).

3. Zeitwert der Intervention der öffentlichen Macht in Bereich der privaten Datenrechte

Aus zivilrechtlicher Sicht soll jedes geschützte Recht das Wesen der Persönlichkeit oder des Eigentums haben. Als Zeichen persönlichen Verhaltens sind Daten zweifellos persönlicher Natur, und Datenrechte werden traditionell als eine Art Recht auf Privatsphäre angesehen, das streng geschützt werden muss.¹⁷ In der Big-Data-Umgebung wird die Eigenschaft des Eigentums an personenbezogenen Daten ständig gestärkt. Angesichts der Krise, in der Rechte der Datensubjekte verletzt werden, kann ihr Schutz nur dann wirksam garantiert werden, wenn entsprechende Rechtshilfemechanismen eingerichtet und perfektioniert werden. Wenn ein Subjekt des Datenrechts meint, dass seine legitime Rechte und Interessen verletzt worden seien oder dass das Verhalten einer Verwaltungsstelle gegen das Gesetz verstoßen habe, hat es das

17 Das „Deliktgesetz der Volksrepublik China“ sieht das Recht auf Privatsphäre in seinen geschützten Bürgerrechten und Interessen vor. Die „Entscheidung des Ständigen Ausschusses des Nationalen Volkskongresses zur Stärkung des Schutzes von Cyberinformationen“ verordnet, dass keine Organisation oder Einzelperson persönlichen digitalen Informationen der Bürger auf rechtswidrige Weise stehlen oder erhalten oder die persönlichen digitalen Informationen der Bürger unrechtmäßig an andere verkaufen oder weitergeben darf.

Recht, einen Antrag auf Wiederprüfung zu stellen oder eine Verwaltungsklage gegen relevante Behörden einzureichen und anzufordern, die Handlungen der Verwaltungsbehörden zu überprüfen. Wenn die rechtswidrigen oder unzulässigen Handlungen von Verwaltungsinstitutionen festgestellt werden, sollen diese widerrufen oder als Verstoß gegen das Gesetz bestätigt werden; und wenn diese Handlungen zur Verletzung der legitimen Rechte und Interessen der Bürger geführt haben, sollte der Verlust der Bürger entschädigt werden. Als hauptsächliche Mittel zur Beilegung von Verwaltungsstreitigkeiten wird Verwaltungsklage in Zukunft eine wichtige Rolle spielen. In der Rechtspraxis in China fallen Verstöße gegen Rechte der persönlichen Daten von Bürgern nicht in den Anwendungsbereich des Verwaltungsrechts. Angesichts der realen Bedürfnisse ist es daher erforderlich, den vorherigen Anwendungsbereich auszudehnen und Fälle wie Verletzung der persönlichen Datenrechte in den Klagebereich aufzunehmen, um Verwaltungsstreitigkeiten im Zusammenhang mit Datenrechten tatsächlich beizulegen und damit die legitimen Rechte und Interessen der Bürger besser geschützt werden können. Es soll beachtet werden, dass Intervention der öffentlichen Macht im Bereich der privaten Datenrechte eine wichtige Ursache für den Missbrauch öffentlicher Macht ist, obwohl sie zum Schutz schwacher Gruppen und zur Wahrung öffentlicher Interessen beitragen kann. Um ihre negativen Auswirkungen zu verringern, ist es daher erforderlich, die öffentliche Macht an sich einzuschränken und den Missbrauch öffentlicher Macht zu verhindern.

Abschnitt IV Schutz der Datenrechte

Die Zuweisung von Datenressourcen und die dadurch verursachten sozialen Probleme sollen dem Grundsatz folgen: „Die mit Technologie gebrachten Probleme sollen vor allem durch Technologie gelöst werden“. Aber die vorhandenen Technologien scheinen keine wirksamen Lösungen bieten zu können. Zu diesem Zeitpunkt ist es notwendig, Lösungen durch Gesetzgebung des Rechtssystems zu suchen (Wen Yuheng 2019). Das Fehlen der Spezifität und Unabhängigkeit von Datenobjekten

sowie die Vermischung der Zerstreutheit und Vielfältigkeit der Subjekte machen es jedoch schwierig, Datenrechte gesetzlich zu zertifizieren. Darüber hinaus erschweren uns die hohen Kosten für die Definition von Datenrechten und viele andere Schwierigkeiten, die auftreten könnten, sobald die Datenrechte gesetzlich festgelegt sind, die Datenrechte als eigenständige Art von Rechten zu errichten. Die realen und komplizierten Streitigkeiten über Datenrechte müssen dringendst gesetzlich entsprechend beigelegt werden und Dateninteressen müssen auch dringendst systemmäßig gewährleistet werden. Eine absolut perfekte Lösung für Datenrechtsschutz ist daher der Aufbau einer Zentrale der technologischen Verwaltung und ständige Verbesserung und Verstärkung von ethischen Richtlinien und Garantie durch Gesetzgebung.

(I) Technologiebasierte Regulierung von Datenrechten

1. Technologiebasierte Regulierung von Datenrechten

Technologie bietet wirksamen Schutz für die Datensicherheit. Man kann sich von 2 Aspekten aus daran arbeiten: Einerseits müssen Staat und Unternehmen mehr Mittel in Forschung & Entwicklung und Innovation investieren, um die Sicherheitsleistung der Cybersysteme und -ausrüstung ständig zu steigern und die Datensicherheit mit fortschrittlicher Technologie zu gewährleisten. Andererseits ist es auch notwendig, Methoden und Modelle aus verschiedenen anderen Bereichen zum Beispiel zu nehmen, um den technologischen Schutz der Datensicherheit vom traditionellen zum modernen Modell reibungslos überzugehen. Daten unterliegen natürlich Codes oder technischen Regeln, sind in Computerterminals oder Speichermedien zu sichern oder zu übertragen. Daher sind technologische Mittel erforderlich, um den Diebstahl von Daten zu verhindern.¹⁸ Einige Wissenschaftler glauben sogar, dass

18 Beispielsweise erhielt der Beklagte Beijing Baidu Netcom Science & Technology Co., Ltd. im Falle von Streitigkeiten über unlauteren Wettbewerb in Bezug auf Beijing Baidu Netcom Science & Technology Co., Ltd. und Shanghai Jietu Software Technology Co., Ltd. die Daten der Kommentare von Online-Nutzern im

„Daten kein Objekt von zivilen Rechten sind, daher kann es kein Recht auf Daten geben, und Daten können nur den Code-Regeln unterliegen. Die Frage des Datenschutzes soll eher auf technologischem als auf rechtlichem Wege gelöst werden“ (Mei Xiaying 2016).

Die Sicherheit der Massendatenspeicherung ist Voraussetzung für Realisierung des Nutzungswerts von Big Data. Wenn Daten in einem Benutzerterminal gespeichert sind, sollte sich der Schutz vom herkömmlichen passiven Schutz zum aktiven Gegenangriff ändern. Traditionell wird das Eigentumsrecht gesetzlich bestätigt, indem die Vorlage eines Eigentumszertifikats zur Überprüfung durch Experten verlangt wird. Es fehlt jedoch die technische Glaubwürdigkeit, und es gibt auch potenzielle unkontrollierbare Faktoren wie Manipulationen. Um diese Probleme zu lösen, besteht ein dringender Bedarf an einem hochgradig funktionsfähigen Eigentumsbestätigungskonzept. Um Risiken wie Datenlecks und Missbrauch etc. vorzubeugen, können wir auf moderne Raketenabwehrsysteme im Militärbereich zurückgreifen. Wir können zeitnahe Sicherheitsanalysen durchführen, um verdächtige Ereignisse zu erkennen und alles zu stoppen, was als gefährliche Rechtsverletzung eingestuft wird, um einen progressiven Schutz der Daten zu verwirklichen. Die technologiebasierte Verwaltung unterscheidet sich von der staatlich zentrierten rechtsbasierten Verwaltung und kann in einigen Fällen sogar einige Einschränkungen für die rechtsbasierte Verwaltung auferlegen.

Die Blockketten-Technologie bietet eine neue Lösungsoption für den Schutz von Datenrechten. Die Blockketten-Technologie, auch als verteilte Hauptbuch(Ledger)-Technologie bezeichnet, besteht aus einer Reihe von Datenblöcken, die mit kryptographischen Methoden korrelativ generiert werden. Es handelt sich um eine neue Anwendung der Computertechnologie wie verteilte Datenspeicherung, Punkt-zu-Punkt-Übertragung, Konsensmechanismus und Verschlüsselungsalgorithmus (He Pu, Yu Ge, Zhang Yanfeng und BaoYubin 2017). Zunächst werden das Auditzentrum und das Wasserzeichenzentrum eingeführt, um die Verantwortung für Prüfung

öffentlichen Kommentarnetzwerk, das vom Kläger Shanghai Hantao Information Consulting Co., Ltd. über Crawler-Technologie betrieben und in seinen Webdiensten wie Baidu Map und Baidu Know (<<https://zhidao.baidu.com> verwendet wird/>). Siehe Shanghai Intellectual Property Rights Court (2016), Hu 73 Minzhong Civil Judgement Nr. 242.

der Integrität von Big Data und die Generierung von Wasserzeichen zu trennen. Zweitens wird eine einfache Prüfung der Big-Data-Integrität auf der Grundlage der Dateninhaber-Bescheinigungs-(Data-Holding-Proof-) Technologie und der Probenahme-(Sampling-)Technologie durchgeführt. Drittens wird die spezielle Sicherheitseigenschaft der digitalen Wasserzeichentechnologie verwendet, um die Herkunft von Big Data zu bestätigen. In Anbetracht der Integrität und Persistenz der Beweise, die am gesamten Prozess der gesetzlichen Rechtsbestätigung beteiligt haben, kann die starke Konsistenz zwischen dem Ergebnis der gesetzlichen Rechtsbestätigung und den relevanten Beweisen unter Verwendung der ursprünglichen Merkmale der Blockketten erreicht werden. Daher kann die Blockketten-Technologie verwendet werden, um Datensicherheitsanforderungen wie Integrität, Beschränkbarkeit und Überprüfbarkeit von Daten zu erfüllen und das grundlegendste Vertrauensproblem der Datenteilhabe zu lösen.

2. Regulierung durch Code-Technologie

Im Zeitalter von Big Data soll die gesetzliche Regelung auf die traditionelle Art der erzwungenen Intervention verzichten und stärkere technologische Strategie und Maßnahmen ergreifen, damit die gesetzliche Regulierung in eine gesetztechnologische Regelung umgewandelt werden kann. Mit der Integrierung, Materialisierung und intelligenten Entwicklung des Internets steuern und regulieren Software und Hardware, die den Cyberspace schaffen, den Cyberspace immer mehr, wo „Kodex Gesetz ist“ (Lawrence Lessig 2009, S. 6). In Bezug auf Bereich wie geistigem Eigentumsrecht, Privatsphäre und Redefreiheit usw. sind Standarderstellung und Codekompilierung neue Regulierungsform und Kontrollkraft. Die Erzeugung, Übersetzung, Übertragung und Speicherung von Daten hängt all von Codes ab. Daten werden auf natürliche Weise durch Codes gesteuert und unterliegen keinen von Codes unabhängigen menschlichen Eingriffen. Codes können eine Reihe von technologischen Regeln generieren, die in „Code“ eingebettet sind. Man kann Codes verwenden, um menschliches Verhalten zu kontrollieren (Zheng Zhihang 2018). Daher kann die Gestaltung der Rechtsstruktur oder der Leistungsverteilung in Bezug auf die Datenordnung durch geeignete Codierung realisiert werden. Im Cyberspace kann sich das Gesetz nicht direkt in den Datenbetrieb an sich einmischen. Die ausdrückliche

Vereinbarung in Verträgen ist bei Weitem weniger effektiv als die automatische Anpassung des Code-Frameworks. „Im Makrohintergrund, wo Daten und Algorithmen zu wichtigen Produktionsfaktoren geworden sind, wird eine große Anzahl von Produktions- und Lebensbeziehungen durch Code erstellt, aufgebaut und aufrechterhalten“ (Ma Changshan 2018). Insbesondere sollen wir aufkommende Rechte und Ansprüche auf rechtliche Interessen im Prozess der Rechtsreform respektieren, da sie den Verhaltenskodex und neue Rechtsbeziehungen in einer Zeit widerspiegeln, in der sowohl der virtuelle als auch reale Raum von Algorithmen dominiert werden und Mensch und Maschine miteinander mischen. Wir sollen technologische Elemente in Aufbau der Rechtsbegriffe und -mechanismen einbeziehen und nach Wegen suchen, um unsere institutionellen Arrangements von einem binären System auf ein integriertes zu verlagern, damit eine neue Rechtsordnung im Zeitalter der digitalen Zivilisation gestaltet werden kann. Das bedeutet natürlich nicht, bestehende Gesetze aufzugeben oder durch etwas anderes zu ersetzen, sondern sie zu erben und weiter zu entwickeln. Tatsächlich ist Code nicht völlig unkontrollierbar. Stattdessen werden die Kompilierung und Änderung der Codes von menschlichen Handlungen geleitet, während die menschlichen Handlungen den gesetzlichen Regeln unterliegen. Somit entsteht eine Brücke zwischen Daten und Gesetzen, das heißt, sie beeinflussen sich einander mittelbar über die Verbindungskette von Gesetz – menschliches Verhalten – Code – Daten (Zhang Yang 2016). Angesichts der Streitigkeiten, die durch Daten an sich verursacht werden (wie Unterschiede in den Eingangswegen der Datenübertragung, mangelnde Vertraulichkeit der Daten und Schwierigkeiten bei der Übersetzung von Datencodes usw.), ist es daher zunächst erforderlich, die technologischen Spezifikationen der Daten zu beachten und den Code für die Regulierung der Datenordnung zu verwenden. Wenn Probleme in Codes auftreten, können Datenrechtsstreitigkeiten gelöst werden, indem das menschliche Verhalten beim Codieren in Übereinstimmung mit Gesetzen geregelt wird.

3. Regulierung der algorithmischen Macht

Daten sind Träger der Informationen und sozialer Interessen. Da die Rechenleistung, die für die Verarbeitung von massiven Daten

erforderlich ist, weit über das hinausgeht, was der Mensch manuell tun kann, muss manuelle Arbeit bei der Zuweisung sozialer Ressourcen allmählich den Algorithmen nachgeben. Unser traditionelles Rechtssystem widmet dem Datenschutz oft mehr Aufmerksamkeit, ignoriert jedoch die Regulierung von Algorithmen. Im Zeitalter der künstlichen Intelligenz erfolgen Datenproduktion und -zirkulation aber auf ganz andere Weise als zuvor, und die Datennutzung birgt neben einem enormen Wert auch große Risiken. „Macht ist ein wichtiger Begriff in der Soziologie und Philosophie. Jede Ressource, über die bestimmte Subjekte genügend verfügen, um andere zu dominieren oder Einfluss auf sie zu üben, kann als Macht genannt werden“ (Jürgen Habermas 1999, S. 76). Als Kraft zur Eroberung und Transformierung der Natur hat Technologie an sich keine Wertorientierung und auch keine Eigenschaft der Macht (Liu Yongmou 2012).

„Wenn die Technologie aber menschliche Interessen direkt beeinflussen und kontrollieren kann, verliert sie ihre Reinheit und hat dann Eigenschaft der Macht“ (Mei Xiaying & Yang Xiaona 2017). Daher bildet die Kraft des Algorithmus zur Ressourcenzuweisung tatsächlich eine Art technologische Macht, die als algorithmische Macht bezeichnet werden kann.¹⁹ Die Fähigkeit, mit der die algorithmische Macht Daten, menschliches Verhalten und Ressourcen der öffentlichen Macht mobilisiert, ermöglicht sie, eine völlig andere Eigenschaft und ganz andere Realisierungsform zu haben. „Sowohl kommerzielle Plattformen als auch der öffentliche Sektor versuchen, den Umfang ihrer Macht durch Einsatz von algorithmischer Kraft zu erweitern und neues Modell der Wissensproduktion und Verwaltung zu erstellen. Aus diesem Grund funktioniert der traditionelle Datenschutzansatz nicht mehr, das Prinzip der Einwilligung nach Auskunft in Bezug auf Schutz personenbezogener Daten war grundsätzlich unwirksam, und der Standard für Qualifizierung der sensiblen personenbezogenen Daten ist durch algorithmische Analyse nahezu bedeutungslos“

19 Algorithmische Macht bezieht sich auf eine neue Art von Macht, die von einigen kommerziellen Organisationen und öffentlichen Institutionen mit Big-Data-Algorithmen erzielt wird.

(Zhang Linghan 2019). Daher erzeugt Algorithmus mittels Daten Wissen, generiert Gewinn und kontrolliert menschliches Verhalten, während das Risiko der Entfremdung der algorithmischen Macht aber auch mit sich gebracht wird.

Die Macht des Algorithmus ist in den Betrieb der öffentlichen Macht auf verschiedenen Ebenen eingebettet und wird in einigen Bereichen sogar zum unabhängigen Entscheidungsträger als Ersatz der öffentlichen Macht. „Aus Sicht der Machtkontrolle folgt das Recht auf Interpretation des Algorithmus im Wesentlichen der Logik der Machtkontrolle – Einschränkung der Macht durch Rechte“ (Zhang Endian 2019). Die „Allgemeine Datenschutzverordnung“ der Europäischen Union befasst sich mit der Regulierung der algorithmischen Macht, indem sie die Transparenz des Algorithmus durch Gewährung von Auslegungsrecht erhöht und die Rechenschaftspflicht der algorithmischen Entscheidungsfindung verbessert. Die Macht des Algorithmus, der verschiedene Bereiche durchquert und stark isoliert ist, übt einen großen Einfluss auf Bereiche wie die Wirtschaft und Politik usw., wobei sie sich dank des „Schleiers“ der Technologie auch von den Zwängen der bestehenden Rechtssysteme befreit werden kann, wodurch die algorithmische Macht weiter gestärkt wird, ohne es bemerkt zu werden. Daher ist es notwendig, unseren Regulierungsansatz in den traditionellen Rechtssystemen rechtzeitig anzupassen, um die Macht des Algorithmus in Schranken zu halten, den Anwendungsbereich von Algorithmen einzuschränken, ordnungsgemäße Verfahrensprozesse und Mechanismen zur Rechenschaftspflicht festzulegen und Rechte der persönlichen Daten und Rechtsschutzmaßnahmen zu gewähren, um einer Verletzung durch Macht des Algorithmus zu widerstehen.

(II) Ethische Regulierung der Datenrechte

1. Ethische Kultur und Schutz der Privatsphäre

Im Allgemeinen bezieht sich Privatsphäre auf den privaten Bereich, der nichts mit öffentlichen Interessen zu tun hat und in dem die Einmischung

durch andere Personen unerwünscht oder inakzeptabel ist.²⁰ Wie Konfuzius es ausdrückte: „Schau nicht auf das, was unanständig ist; höre nicht auf das, was unanständig ist; sprich nicht, was unanständig ist; mach keine Bewegung zu dem, was unanständig ist.“ Anstand bedeutet hier Etikette und Riten. Man sollte es unterlassen, etwas zu tun, was der Angemessenheit widerspricht; man soll an sich halten, darf nicht absichtlich nach den Geheimnissen anderer Menschen erkundigen. Man soll Dinge im Einklang mit dem Anstand tun und die Privatsphäre anderer respektieren. Das ist die traditionelle Doktrin zur Privatsphäre im Konfuzianismus. Man kann sagen, dass Anstand ein zentrales Konzept in der traditionellen chinesischen Kultur ist und sich durch die gesamte alte chinesische Gesellschaft zieht. Die gegenseitige Durchdringung und Integration von Anstand und Recht hat der traditionellen chinesischen Rechtskultur klare ethische Merkmale verliehen. Die Konfuzianischen moralischen Grundprinzipien im alten China bilden die theoretische Grundlage für die Entwicklung des chinesischen Rechtssystems und „so entstand die ethischen Gesetze mit chinesischen Merkmalen, die durch enge Kombination von Recht und

20 Die Weltprivatsphäreorganisation ist der Ansicht, dass der Begriff der Privatsphäre mit dem Datenschutz, also mit der Verwaltung persönlicher Informationen verbunden ist. „Unter allen internationalen Kategorien in Bezug auf Menschenrechte ist es am schwierigsten, die Privatsphäre zu definieren. Aufgrund der verschiedenen Hintergründe und Umgebungen ändert sich die Definition der Privatsphäre auch sehr unterschiedlich. Das Recht auf Privatsphäre wird in vier Arten aufgeteilt, die unabhängig voneinander und auch verbunden miteinander sind, einschließlich Informationsprivatsphäre, Körperprivatsphäre, Kommunikationsprivatsphäre und Ortsprivatsphäre. Darunter deckt die Informationsprivatsphäre das entsprechende System für Regelung der Sammlung und Verfügung von personenbezogenen Daten, wie z.B. Kreditinformationen und medizinische Informationen. Als Verwalterin und Dienstleisterin der Gesellschaft ist die Regierung auch die größte Verbraucherin der persönlichen Daten der Bürger. Zweifellos verfügen Bürger über das absolute Recht auf persönlichen Informationen. Die Regierung darf nicht das Verfügungsrecht auf die persönlichen Informationen der Bürger haben, selbst wenn sie diese besitzt. Sie soll dabei von den Bürgern eingeschränkt und kontrolliert werden. Das Recht auf persönliche Informationen und Privatsphäre manifestiert sich schließlich in Schutz der Menschenrechte, deren Schutz durch Gesetzgebung rechtstheoretisch legitim und unweigerlich ist und deren Rechtsstellung auch unerschütterlich ist“.

Moral gebildet ist“ (Zhang Jinfan 2009, S. 113–129). Mit anderen Worten, die Grundlage der alten chinesischen Gesetze ist die konfuzianische „Ethik und Moral“. Tatsächlich muss jedes Land seine eigene Wertorientierung, die Geschichte seines Rechtssystems und die Entwicklungsgeschichte seiner Rechtsgedanken berücksichtigen, wenn es seine eigenen Gesetze verabschiedet, einschließlich derer zum Schutz der Privatsphäre. Mit der rasanten Entwicklung von Wissenschaft und Technologie im 20. Jahrhundert trat die menschliche Gesellschaft ins Informationszeitalter ein, wo die Menschen auch ihre Kommunikationsweise veränderten. Das hat die Themen wie Informationssicherheit und Schutz der Privatsphäre usw. zum Schwerpunkt der sozialen Aufmerksamkeit gemacht. „Eine der ethischen Grundlagen des Schutzes der persönlichen Daten ist der Schutz der Menschenwürde und die Verhinderung der Objektivierung von Personen durch Informatisierung der persönlichen Daten“ (Guo Yu 2012, S. 83–84). Die Entstehung und Entwicklung von Persönlichkeitsrechten ist eng mit der ethischen Kultur verbunden. Jeder hat Würde und Zweck des Rechts auf Privatsphäre ist es, die Menschenwürde, Freiheit und Unabhängigkeit der Persönlichkeit zu schützen. Die ethische Kultur hat nicht nur einen wichtigen Einfluss auf das System des Datenrechtsschutzes, sondern spielt auch eine wichtige Rolle im Justizbereich in China. In der spezifischen Rechtspraxis werden ethische Standards normalerweise verwendet, um gesetzliche Unklarheiten oder Konflikte zu interpretieren, um die Urteile den sozialmoralischen Standards zu entsprechen. In Hintergrund der gegenwärtigen Ära von Big Data soll die Regierung das Rechtssystem zum Schutz der Privatsphäre einrichten und verbessern, damit in relevanten Fällen Gesetze eingehalten werden können. Als Datensammler sollen Unternehmen einerseits Kundendaten gesetzeskonform verwenden und andererseits ihre Schutzfähigkeit für Datensicherheit erhöhen. Darüber hinaus sollen Bürger eine korrekte Ansicht auf die Privatsphäre hinstellen.

2. Moralische Selbstregulierung der Branche

„Der moralische Charakter ist ein gewohnheitsmäßiger, stabiler, dauerhafter und psychologischer Gesamtzustand einer Person, die sie in ihrer langfristigen und einer Reihe von Verhaltensweisen aufweist“ (Wang Haiming 2009, S. 373). Ein guter moralischer Charakter ist von großem Nutzen für

die Entwicklung der menschlichen Gesellschaft, während ein „schlechter moralischer Charakter“ seine Schädlichkeit für die Gesellschaft unvorstellbar sein könnte. Die Pflege eines guten moralischen Charakters ist ein langer Prozess. Es ist dringend erforderlich, die Pflege einer guten Moral der Datenbeteiligten im Zeitalter von Big Data zu stärken. Im Cyberspace, in dem die ethisch-moralischen Regeln relativ schwach und rückständig sind, wird die Big-Data-Technologie eher in großem Umfang angewendet. Wenn die moralische Selbstregulierung der Dateninteressenbeteiligten nicht gestärkt würde, könnte die Entfremdung der Technologie nicht in Kontrolle gehalten werden, und die daraus entstehenden Folgen könnten katastrophal sein und über unsere Vorstellungskraft hinausgehen. Es könnte sogar zu der Illusion führen, dass der „schlechte moralische Charakter“ zum Normalzustand im Zeitalter von Big Data geworden wäre. Das heißt, sobald Dateninteressenteilhaber einen stabilen „schlechten moralischen Charakter“ gebildet hätten, würde der „gute moralische Charakter“ aber zur Abnormität und bestünde dann ein großes Risiko für Entfremdung der Big-Data-Technologie.

Der amerikanische Gelehrte Richard A. Spinello schlug drei Prinzipien der cyberethischen Normen vor und wies darauf hin, dass „Technologie sich tendenziell schneller entwickelt als Ethik, und der Verzögerungseffekt in diesem Aspekt wird uns erheblichen Schaden zufügen“.²¹ „Im Vergleich zu

21 Das Erste ist das Prinzip der Autonomie. Autonomie bedeutet, dass Einzelperson die Möglichkeit hat, ihre eigene Lebensweise zu bestimmen. Wenn diese Idee mit personenbezogenen Daten kombiniert wird, haben Dateneigentümer das Recht zu entscheiden, in welchem Bereich ihre personenbezogenen Daten angewendet werden können und welcher Wert erzielt werden kann. Das Zweite ist das Prinzip der Harmlosigkeit. Wenn moderne Technologie verwendet wird, um personenbezogene Daten zu verarbeiten und einen entsprechenden Wert zu erzielen, kann dies den Dateneigentümern keinen Schaden zufügen. Das ist einer der Ansätze zum Schutz personenbezogener Daten. Das Dritte Prinzip besteht im Grundsatz der Einwilligung nach Aufklärung. „Zustimmung“ ist der Ausdruck des subjektiven Willens der Menschen, bei dem die betroffenen Personen die Art und den Zweck der Datenverarbeitung klar verstehen müssen, d.h. unter der Voraussetzung des Informiert-Werdens. Siehe Richard A. Spinello: „Ethik des Jahrhunderts: die ethischen Aspekte der Informationstechnologie“, Trans. Liu Gang. In Peking: Zentrale Zusammenstellungs- und Übersetzungspresse, 1998.

den gesetzlichen Bestimmungen können Selbstregulierungsnormen einen „endogenen Mechanismus“ etablieren, damit die Kosten der staatlichen Regulierung wirksam gesenkt werden“ (Lu Li 2003, S. 190–193). In der „Allgemeinen Datenschutzverordnung“ der Europäischen Union wurde das Konzept eingeführt: Die Branche spielt eine führende Rolle und die Regierung muss nur moderate Beschränkungen auferlegen. Oder anders ausgedrückt: Auf der Makroebene reguliert und formuliert die Regierung grundlegende Rahmenbedingungen und Grundsätze für Schutz persönlicher Daten, während der Markt die grundlegende Rolle der Selbstverwaltung auf Mikroebene spielt. Anders als die von der Europäischen Union verabschiedeten umfassenden Rechtsvorschriften stützen sich die Vereinigten Staaten auf die Branchenselbstregulierung, um personenbezogene Daten im privaten Bereich zu schützen. In den Vereinigten Staaten bilden neben spezifischen Bundesgesetzen, Landesgesetzen und allgemeinen Gesetzen in einigen Bereichen die von Nichtregierungsorganisationen und Unternehmenssitzungen erlassenen internen Arbeitsvorschriften auch einen wichtigen Bestandteil der Normen für den Schutz personenbezogener Daten (Qi Aimin 2015, S. 89).

Derzeit gibt es in China kein spezielles Gesetz zum Schutz personenbezogener Daten. Personenbezogene Daten sind vor allem durch Abteilungsgesetzgebung in verschiedenen Bereichen geschützt. Jetzt befindet sich die Branchenselbstregulierung erst in der Anfangsphase, und Branchenvorschriften zum Schutz personenbezogener Daten sind auch ganz selten (Zhang Jihong 2018). Daher müssen wir der Selbstregulierung von Industrieverbänden auf der Grundlage einschlägiger Rechtsvorschriften einen größeren Spielraum geben und alle Industrieverbände ermutigen, sich aktiv an der Formulierung und Umsetzung von Bestimmungen für Verhaltenskodex zum Datenschutz zu beteiligen und einen Selbstregulierungsmechanismus auf der Grundlage der objektiven Branchenbedürfnisse „von unten nach oben“ zu bilden. Darüber hinaus sind staatliche Leitlinien und Anweisungen erforderlich, um eine organische Synergie zwischen angemessener staatlicher Aufsicht und Branchenselbstregulierung zu schaffen und die reale Wirksamkeit des Datenschutzes schrittweise zu verbessern.

3. Regulierung des ethischen Systems

„Gerechtigkeit ist der Hauptwert des sozialen Systems“ (John Rawls 1988, S. 11). Das derzeitige ethische System ist jedoch nicht ganz gerecht, da ein für die Vergangenheit geeignetes ethisches System für die heutige Ära von Big Data möglicherweise nicht geeignet ist. Dies erfordert, dass wir auf die Meta-Ethik der Gerechtigkeit und ihre Verwirklichung im ethischen System der modernen Gesellschaft achten. Daher müssen wir einerseits die relevanten ethischen Systeme verbessern, damit sie dazu beitragen können, die negativen Folgen der Entfremdung der Big-Data-Technologie zu beseitigen, und uns bemühen, die Gerechtigkeit der relevanten ethischen Systeme an sich zu gewährleisten, d.h. bei der Gestaltung in Bezug auf relevante ethische Systeme müssen wir uns darauf konzentrieren, wie Entmenschlichung, Nicht-humanismus und Nichtliberalisierung im Zeitalter von Big Data beseitigt werden können. Andererseits müssen wir spezifische Normen des ethischen Systems für Dateninteressenbeteiligte formulieren, um sicherzustellen, dass die relevanten ethischen Systeme selbst gerecht sind. So ist es erforderlich, praktische und realisierbare Normen des ethischen Systems für Dateninteressenbeteiligte zu erstellen, damit die Big-Data-Technologie in der Gesellschaft auf gesunder Weise zur Geltung gebracht werden kann (Chen Shiwei 2016).

Datensicherheit ist nicht nur ein technisches Problem, sondern auch ein Kompromiss zwischen Interessen, Werten und Ethik. Gemäß dem „Plan zur Einrichtung des Nationalen Ethikausschusses für Wissenschaft und Technologie“, der vom Zentralkomitee der KP Chinas für umfassende Vertiefung der Reformen überprüft und verabschiedet wurde, müssen institutionelle Normen vervollständigt, Verwaltungsmechanismen verbessert, die ethische Aufsicht verstärkt, relevante gesetzliche Vorschriften und Bestimmungen und Regeln für ethische Überprüfung verfeinert und verschiedene Arten von Forschungsaktivitäten spezifiziert werden“. Auf der vierten Plenartagung des 19. Zentralkomitees der KP Chinas wurde vorgeschlagen, das „Verwaltungssystem der Wissenschafts- und Technologieethik zu verbessern“. Und „Privatsphäre kann nicht bloß als Geheimhaltung, sondern auch als Regelwerk der Ethik und Moral für Erfassung und Offenlegung persönlicher Informationen verstanden werden (Wu Weiguang 2016). Aus analytischer Sicht der institutionellen Ethik besteht die ethische Verwaltung des Datenschutzes im Zeitalter der digitalen Zivilisation darin,

ethische Normen einzuhalten. In der sozialen Verwaltung durch Kooperation der privaten Rechte und öffentlicher Macht sollen die Institutionen der öffentlichen Macht die Kontrolle behalten, um eine neue Ordnung der Moral-Ethik und des sozialen Wettbewerbs zu gestalten, wobei der Schwerpunkt auch auf Schulung und Ausbildung von Mitarbeitern in Bezug auf Regeln der datenbezogenen Ethik und Standards der moralischen Verantwortung gelegt werden soll.

Im Wissenschaftskreis wird allgemein angenommen, dass relevante ethische Prinzipien für die ethischen Probleme festgelegt werden sollen, die durch die Big-Data-Technologie verursacht werden: Das Erste ist das Prinzip der Harmlosigkeit. Das heißt, bei der Entwicklung der Big-Data-Technologie soll man immer auf Menschen ausgerichtet sein, um der gesunden Entwicklung der menschlichen Gesellschaft zu dienen und die Lebensqualität der Menschen zu steigern. Das Zweite ist die Einheit von Rechten und Pflichten. Das heißt, wer Daten sammelt, der trägt die Verantwortlichkeit dafür; wer Daten verwendet, soll auch dafür verantwortlich gemacht werden. Das Dritte ist das Prinzip der Achtung der Autonomie, d.h. das Recht auf Speicherung, Löschung, Nutzung von Daten und das Recht auf Informiertheit sollen den Datenproduzenten uneingeschränkt gewährt werden (Yang Weidong 2018). Aus historischen Gründen wurden Unternehmensgruppen mit starker Selbstregulierung und ethischen Normen in China noch nicht vollständig gebildet, sodass wir uns nicht so sehr wie in den USA auf Branchenselbstregulierung verlassen können. Das zwingt die Regierung, die Rolle als Gestalterin von Datensystem, Gesetz und Moral zu spielen.

(III) Gesetzlicher Schutz der Datenrechte

1. Notwendigkeit des gesetzlichen Schutzes der Datenrechte

„Das Gesetz ist keine abstrakte mechanische Regel. Es trägt sondern bestimmte soziale Werte und spiegelt den Verhaltenskodex und die Lebenserfahrungen der Menschen wider“ (Ma Changshan 2018). Daher kann man beim Aufbau des Gesetzes die soziale Realität nicht ignorieren. Die gesetzliche Anpassung muss auf den tatsächlichen Bedürfnissen der Gesellschaft beruhen. Die Funktion der gesetzlichen Vorschriften fordert

an, dass wir ein Schutzsystem für Datenrechte einführen, das der sozialen Entwicklung entspricht. In der heutigen Gesellschaft verfolgen Datensubjekte tendenziell immer mehrere und vielfältigere Ansprüche auf Datenrechte und -interessen und schwärmen dafür, neue Interessenansprüche als neue Arten von Rechten qualitativ zu definieren. Sie rufen sogar auf, ihre Ansprüche in Form der Gesetzgebung klar zu schützen. Einzelpersonen (Benutzer) und Unternehmen machen aufgrund ihrer eigenen Interessen unterschiedliche Ansprüche geltend. Tief im inneren Sinne ist es der Wettbewerb zwischen den Rechten auf personenbezogene Daten und der Datennutzung durch Unternehmen und der Wettbewerb zwischen Unternehmen um das Recht auf Datenkontrolle. Es ist auch ein Durchbruch und eine Überarbeitung des bestehenden stabilen Rechtssystems, nachdem die Liste der datenbezogenen Rechte erweitert und verfeinert wurde. Aufgrund des unterschiedlichen sozialen Hintergrunds der Datensubjekte unterscheiden sich ihre Ansprüche auf Dateninteressen erheblich und zeigen einen offensichtlichen Trend der Interessendifferenzierung. Das Abwägen und Koordinieren zwischen den Datenrechten und -interessen von Einzelpersonen, Unternehmen und der Öffentlichkeit ist daher nicht nur eine neue Aufgabe unseres Justizsystems, sondern auch ein Test für die Weisheit des Gesetzgebers (Li Xiaoyu 2019). Seit dem 21. Jahrhundert sind in vielen Ländern die Arbeiten zur Gesetzgebung über Daten in vollem Gange, und China beschleunigt auch seine Fortschritte im Bereich der Gesetzgebung für Schutz persönlicher Information.²² Aus Sicht der vorhandenen Gesetzgebungsbestimmungen scheint es bisher keine spezifischen gesetzlichen Bestimmungen zu Rechten an Unternehmensdaten zu geben und solche Rechte können nur durch das „Gesetz der Volksrepublik China gegen unlauteren Wettbewerb“ geschützt und geregelt werden. Gleichzeitig erfordert die Verwaltung und Offenlegung von Regierungsdaten eine solide Systemreihe, insbesondere ist es erforderlich, entsprechende technische Standards und Vorschriften dazu zu erstellen. Wir sollten ein tiefes Verständnis für den internationalen Gesetzgebungstrend im Zusammenhang mit dem Datenschutz haben, wirksame Maßnahmen

22 In dem im September 2018 veröffentlichten Legislativplan des Ständigen Ausschusses des 13. Nationalen Volkskongresses steht das Gesetz zum Schutz personenbezogener Daten auf Platz 61 der Tagesordnung.

zum Datenschutz ergreifen und ein angemessenes Rechtssystem für diesen Zweck aufbauen.

2. Zwangslage der Legalisierung von Datenrechten

Ob die Datenrechte gesetzlich festgelegt werden können oder nicht, bedarf sorgfältiger logischer Rechtfertigung. Tatsächlich gibt es viele Hindernisse auf dem Weg zur Legalisierung der Datenrechte, sowohl mit deduktiver Vorwärtsargumentierung als auch mit hypothetischer Rückwärtsschlussfolgerung (Zhang Yang 2016). Während des ganzen Prozesses der Erfassung und Verwendung von Kundendaten könnten Internetunternehmen Datenrechte verletzen. Es ist jedoch sehr schwierig, diese mit dem Deliktsgesetz zu regeln, da die Datenerfassung und -analyse auf eine Weise erfolgt, die für außenstehende Kunden unsichtbar ist. Selbst wenn Kunden den Verdacht haben, dass ihre Rechte verletzt worden sind, wissen sie möglicherweise nicht, wen sie anklagen sollen, oder es fehlen die erforderlichen Beweise, um jemanden zur Verantwortung zu ziehen oder Schadensersatz zu beanspruchen. Darüber hinaus ist das Dateneigentumsrechtssystem das Produkt einer staatlichen Regulierung des Datenverkehrs. Es müssen jedoch praktische Anpassungen entsprechend der sozialen Effizienz vorgenommen werden, um den Interessenausgleich zwischen Datennutzern, Datenverarbeitenden und der Öffentlichkeit zu gewährleisten. Das ultimative Ziel besteht darin, einen ausgewogenen und gut koordinierten Mechanismus für die Verteilung von Datenrechten und -interessen zu schaffen, der die ordnungsgemäße Verwendung von Daten durch alle Interessenbeteiligten gewährleistet. Es gibt jedoch immer noch viele Mängel beim rechtlichen Schutz der Datenrechte in China. Erstens mangelt es an juristischer Forschung. In den „Allgemeinen Bestimmungen des Zivilrechts“ und anderen einschlägigen Gesetzen wurden die entsprechenden Maßnahmen zum Datenschutz erwähnt. Im Wesentlichen gibt es aber keine spezifischen Bestimmungen zur Definition, Art und Struktur von Datenrechten, die den aktuellen Bedürfnissen der Bürger nach Schutz ihrer Datenrechte nicht gerecht werden können. Zweitens mangelt es an verfassungsrechtlicher Unterstützung. Die Verfassung der Volksrepublik China betrachtet Rechte an personenbezogenen Daten nicht ausdrücklich als eine Art Schutzrecht wie viele andere Arten von Rechten. Außerdem gibt es in China kein spezielles Gesetz zum

Schutz personenbezogener Daten. Der Schutz der Rechte auf personenbezogene Daten ist vereinzelt und unklar. Darüber hinaus betonen einige Zivilrechtswissenschaftler die Rechte der Datensubjekte, wie das Recht auf Informiertheit, das Recht auf Zugang, das Recht auf Berichtigung, das Recht auf Datenmitnehmbarkeit und das Recht auf Vergessen von Daten usw. Selbst mit ausdrücklicher persönlicher Zustimmung können Unternehmen das Recht zur Kontrolle personenbezogener Daten nicht in vollem Umfang genießen, und müssen die Grundrechte der Datensubjekte bei der Erhebung, Behandlung und Verarbeitung ihrer persönlichen Daten gewährleisten (Shi Dan 2019). Gleichzeitig sollen Unternehmen und Regierungen die Transparenz der Big-Data-Anwendung verbessern, die Öffnung und Teilhabe von Unternehmensdaten und Regierungsdaten ermuntern und die Entwicklung und Nutzung von Datenprodukten fördern. Der Schlüssel zum Gleichgewicht zwischen den Datenrechten und der Entwicklung der Datenindustrie besteht darin, die Befugnisse der Unternehmen zur Nutzung und Verarbeitung von Daten zu klären. Die Bestimmungen zum Schutz der Datenrechte in China sind jedoch nicht spezifisch und nicht konkret. Und diese Datenrechte werden sogar nicht als eine unabhängige Kategorie von Rechten festgelegt und geschützt.

3. Aufbau des Systems zum Datenrechtsschutz

Beim Schutz der Datenrechte können wir uns nicht nur einseitig auf den Schutz der Rechte und Interessen bestimmter Subjekte konzentrieren, sondern auch im Blickwinkel des Interessengleichgewichts die Datenbeziehungen zwischen verschiedenen Rechtssubjekten wie Einzelpersonen, Unternehmen und Regierungen koordinieren und anpassen. Als Verhaltenskodex für Anpassung der sozialen Beziehungen soll und kann das System zum Datenrechtsschutz eine Rolle für Beilegung von Streitigkeiten bei Interessenverteilung in einer Gesellschaft mit komplexen Datenbeziehungen spielen. Daher ist es beim Aufbau eines Systems zum Datenrechtsschutz erforderlich, den Status der Regierung, der Unternehmen und Einzelpersonen im Datenrechtsverhältnis klarzustellen, die Konnotation und Grenze der Datenrechte zu definieren, die Rechts- und Pflichtbeziehungen zwischen den Datenrechtsinhabern und Datenbenutzern angemessen festzulegen, einen typisierten und klassifizierten Schutz

basierend auf den Datentypen durchzuführen und schließlich ein Gesetz und System zur gesetzlichen Bestätigung der Datenrechte zu formulieren, das sowohl unseren nationalen Bedingungen entspricht als auch mit den internationalen Standards im Einklang steht (Zhu Lei 2019).

Erstens soll das persönliche Datenrecht als ein Grundrecht geschützt werden. In Artikel 8 der Charta der Grundrechte der Europäischen Union²³ heißt es: „Jeder hat das Recht auf Schutz personenbezogener Daten, die ihn betreffen“. Diese Daten müssen für bestimmte Zwecke und auf der Grundlage der Zustimmung der betreffenden Person oder einer anderen gesetzlich festgelegten legitimen Basis fair verarbeitet werden“. Daraus ist ersichtlich, dass die Europäische Union den Schutz personenbezogener Daten fördert, indem sie die Rechte auf personenbezogene Daten als Grundrechte festlegt, die die Kategorie von Rechten darstellen, die im Rechtssystem der Europäischen Union am besten geschützt sind. China soll die Gesetzgebung zum Schutz der Datenrechte beschleunigen, um die „persönlichen Datenrechte“, die als eine Art unabhängiges und grundlegendes Bürgerrecht anerkannt sind, direkt zu schützen.

Zweitens soll das Schutzsystem für grundlegende Datenrechte und -interessen unter Bezugnahme auf andere Vorgehensweise für Rechtsschutz eingerichtet werden. Die Datenrechte besitzen nicht nur die Eigenschaft der Datenrechte und -interessen wie Offenheit und Teilhabe etc., sondern auch einige Merkmale von Eigentumsrecht, geistigem Eigentumsrecht und Persönlichkeitsrecht. Diese Eigenschaften und Merkmale zusammen

23 Die „Charta der Grundrechte der Europäischen Union“ unterscheidet sich von den traditionellen Rechtsdokumenten der Menschenrechte wie der „Europäischen Menschenrechtskonvention“ darin, dass sie kein universelles und unabhängiges Menschenrechtsgesetz ist: Sie wird nur angewendet, wenn die EU-Institutionen und die Mitgliedstaaten die EU-Gesetze umsetzen. Die Gesetze der EU und der EU-Mitgliedstaaten stehen im Einklang mit der „Charta der Grundrechte der Europäischen Union“ und nehmen diese als Mindestanforderung an. Die Bestimmungen der Gesetze der EU und der EU-Mitgliedstaaten, die im Widerspruch zur „Charta der Grundrechte der Europäischen Union“ stehen, dürfen nicht angewendet werden. Siehe Menno Mostert, Annelien L., Bredenoord, Bartvander Sloot, Johannes J. M. van Delden. 2017. „Vom Datenschutz zum Datenschutz in der Europäischen Union: Auswirkungen auf die Big Data-Gesundheitsforschung.“ *European Journal of Health Law*, 25. Ausgabe.

machen es unmöglich, ein System zum Schutz der Datenrechte aufzubauen, das nur einer bestimmten Rechtstypen in unseren bestehenden Systemen entspricht (Deng Ganghong 2018). Zum Thema der Definition des Dateneigentumsrechts sollen die Bestimmungen an die im aktuellen Rechtssystem definierten Rechtsschutzsysteme angepasst werden und andere ähnliche Eigentumsrechtssysteme zum Beispiel genommen werden.

Schließlich ist es notwendig, alle Arten neuer komplexer Beziehungen im Zeitalter von Big Data richtig zu handhaben. Zum einen muss der Zusammenhang zwischen der Datenerfassung durch Regierungsstellen und dem Schutz personenbezogener Daten geklärt werden. Unter Berücksichtigung der Sicherheit und Interessen des Staates sollen persönliche Datenrechte teilweise übertragen werden. Die Regierung sollte sich jedoch bei der Erhebung persönlicher Daten strikt an die gesetzlichen Verfahren halten sowie den Zweck und Anwendung klarstellen. Zum anderen soll eine klare Grenze zwischen den Rechten an Unternehmensdaten und dem Schutz personenbezogener Daten gezogen werden. Die Big Data in der Hand von Unternehmen werden im Wesentlichen aus personenbezogenen Daten abgeleitet. Einerseits sollen Persönlichkeitsinteressen wie die Privatsphäre geschützt werden; andererseits sollen auch die Datenrechte von Unternehmen ausreichend geschützt werden, insbesondere die nach Anonymisierung und Desensibilisierung entstandenen Big Data, deren Eigentumsrechte auch genügend geschützt werden sollen (Song Jianbao 2019). Drittens könnten Regierungen, Unternehmen oder Einzelpersonen die Rechte der Bürger auf personenbezogene Daten verletzen. Dementsprechende Hilfsmaßnahmen müssen verfügbar sein, unabhängig davon, welche Art von Verletzung auch vorliegt.

Literaturverzeichnis

- Beck, Deng Zhenglai & Shen Guolin: „Risikogesellschaft und China - Dialog mit dem deutschen Sozialwissenschaftler Ulrich Beck“, in „Forschung über Sozialwissenschaft“, 5/2010.
- Bertrand Russell: „Einführung in die mathematische Philosophie“, übersetzt von Yan Chengshu, Die kommerzielle Presse, 1982.

- Chen Hongzhi: „Erste Forschung über den Eintritt des Privatrechts in Bereich des öffentlichen Rechts“, in „Rechtsstaatlichkeit und Gesellschaft“, 2/2018.
- Chen Shanglong: „Forschung über Gesetzgebung zu Öffnung der Regierungsdaten im Zeitalter von Big Data“, in „Forschung über lokale Gesetzgebung“, 2/2019.
- Chen Shiwei: „Ethische Regulierung der Entfremdung von Big-Data-Technologie“, Studien zur Dialektik der Natur, 1/2016.
- Chen Zhentao: „Kompetenzstruktur und Analyse der Rechtsposten des persönlichen Informationsrechts“, in „Fujian Rechtswissenschaft“, 1/2017.
- Cheng Xiao: „Über das Recht auf personenbezogenen Daten im Big Data Zeitalter“, in „Chinesische Sozialwissenschaft“, 3/2018.
- „Cybersicherheitsgesetz der Volksrepublik China“, Art. 76.
- Deloitte und Ali Forschungsinstitut: „Der Weg zur Datenkapitalisierung – Bewertung von Datenvermögen und Branchenpraxis“, <<https://www2.deloitte.com/cn/zh/pages/finance/articles/data-asset-report.html>>, 29. Oktober 2019.
- Deng Ganghong: „Gesetzlich logische Analyse der Attribute von Big-Data-Rechten: Der Schutzansatz für Rechte an personenbezogenen Daten“, Jianghai Academic Journal, 6/2018.
- Dong Zhiwei: „Recht und Verfassung“, Volksverlag Shandong, 2001.
- EU: „Allgemeine Datenschutzverordnung“, Art. 4 Abs. 1 (GDPR).
- Gao Jianping u. Qi Zhiyuan: „Big Data und Wiederaufbau der gegenwärtigen Sozialordnung“, in Forschung über Dialektik der Natur, 5/2019.
- Guo Yu: „Forschung über Schutzrecht auf personenbezogene Daten“, Peking University Press, 2012.
- Hangzhou Railway Transportation Court (2017) Zhe 8601 Zivilurteil Nr. 4034.
- Hans Brocks & Wolff Dietrich Walker: „Überblick über das deutsche Bürgerrecht“, 41. Ausgabe, übersetzt von Zhang Yan, Verlag der chinesischen Remin Universität, 2019, S. 276.
- Hao Jiming: „Entfremdung der öffentlichen Macht und ihre Kontrolle“, in „Kreuz und quer durch Sozialwissenschaften“, 7/2008.
- He Dingding: „Wie soll die Datenmacht die Kundenrechte und -interessen respektieren“, in Volkszeitung, 23. März 2018.
- He Pu, Yu Ge, Zhang Yanfeng u. Bao Yubin: „Zusammenfassung der Blockkettentechnologie und Anwendungsvorschau“, in „Computerwissenschaft“, 4/2017.
- Hu Ling: „Über Code hinaus: Kontroll-Produktionsmechanismus vom Cyberspace zur physischen Welt“, in Journal der Huadong Universität der Politikwissenschaft und Rechtskunde, 1/2018.
- Huang Ruhua, Wen Fangfang u. Huang Wen: „Über den Aufbau des Richtliniensystems für Öffnung und Teilhabe der Regierungsdaten unseres Landes“, in „Bibliotheksinformationsarbeit“, 9/2018.
- Jiao Shiwen: „Philosophische Forschung über Umwandlung der Machtstruktur in China“, Parteihochschule des ZK der KP Chinas, Doktorarbeit, 2009.

- John Rawls: „Eine Theorie der Gerechtigkeit“, übersetzt von He Huaihong et al. Der Chinesische Sozialwissenschaftliche Verlag, 1988.
- Jürgen Habermas: „Technologie und Wissenschaft als ‚ideologische Vorstellung‘“, übersetzt von Li Li, Guo Guan, Xuelin Verlag, 1999.
- Kalin Hristov, „Artificial Intelligence and Copyright Dilemma“, IDEA: The IP Law Review, 2017 (57).
- Kang Xiaoguang: „Übergabe der Macht - Veränderungen der chinesischen Machtstruktur in der Periode der Transformation“, 1999.
- Kevin Kelly: „Technische Elemente“, übersetzt von Zhang Xingzhou et al. Verlag der Elektron-Industrie, 2012.
- Lawrence Lessig: „Code 2.0: Gesetz im Cyberraum“, übersetzt von Li Xu u. Shen Weiwei, Tsinghua University Press, 2009, S. 6.
- Li Xiaoyu „Typisierter Schutz von Datenrechten und -interessen aus der Perspektive der Unterscheidung zwischen Rechten und Interessen“, in Geistes Eigentumsrecht, 3/2019.
- Li Yang u. Li Xiaoyu: „Abgrenzung der Eigenschaft der Rechte und Interessen der Unternehmensdaten und Struktur ihres Schutzmodells im Zeitalter von Big Data“, in „Profunde Kenntnisse“, 4/2019.
- Lin Qifu u. He Jingchao: „Macht von Big Data: eine moderne Machtlogik und Reflexion über ihre Erfahrung“, in Journal der Nordosten Universität, Sozialwissenschaften, 5/2016.
- Liu Hong u. Hu Xinhe: „Datenrevolution: historische Erforschung von Zahl zu Big Data“, in „Nachrichtenübermittlung der Dialektik der Natur“, 6/2013.
- Liu Jiangang: „Zertifizierung der Datenrechte“, in Journal der Berufshochschule der Politologie und Rechtskunde, 4/2016.
- Liu Yongmou: „Maschine und Herrschaft – Machtdimension der Marx Theorie über Wissenschaft und Technik“, in „philosophische Studie der Wissenschaft und Technik“, 1/2012.
- Long Weiqiu: „Forschung über Aufbau des neuen Dateneigentumsrechts und seines Systems“, in „Rechtskunde im Osten“, 4/2017.
- Long Weiqiu: „Nochmal über den Weg der Legalisierung des Eigentumsrechts für Unternehmensdatenschutz“, in „Rechtskunde im Osten“, 3/2018.
- Lu Li: „Forschung über Wirtschaftsautonomie der Branchenvereine“, Rechtsverlag, 2003.
- Lü Tingjun: „Datenrechtssystem und seine rechtstaatliche Bedeutung“, in Journal Parteihochschule des Zentralkomitees der KP Chinas, 5/2017.
- Lü Zhixiang u. Zhang Qiang: „juristische Analyse der Datenrechte im Hintergrund der Big Data“, in Journal Universität der Naturwissenschaft und Technik Kunming, „Sozialwissenschaft“, 1/2019.
- Ma Changshan: „Rechtsreform im Zeitalter des intelligenten Internets“, in Chinese Journal of Law, 4/2018.

- Mei Xiaying u. Yang Xiaona: „Entstehung und Regelungsweg der Cybermacht auf Eigenmedien-Plattform – Analyse von Einfluss auf die Cyber-Redefreiheit“, in „Hebei Rechtskunde“, 1/2017.
- Mei Xiaying: „Gesetzliche Eigenschaft der Daten und ihre Positionierung im Zivilrecht“, in „Chinesische Sozialwissenschaften“, 9/2016.
- Qi Aimin u. Pan Jia: „Grundregeln für Festlegung von Datenrecht und Datensouveränität sowie Schutz von Big Data“, in „Journal Suzhou Universität“, „Philosophie und Sozialwissenschaft“, 1/2015.
- Qi Aimin: „Forschung mit internationalem Vergleich über Schutzrecht für personenbezogene Daten im Zeitalter von Big Data“, Rechtsverlag, 2015.
- Richard A. Spinello: „Ethik des Jahrhunderts: die ethischen Aspekte der Informationstechnologie“, übersetzt von Liu Gang. Zentrale Zusammenstellungs- und Übersetzungspresse, 1999.
- Ru Xin: „Geschichte der westlichen Ästhetik“, Verlag der chin. Sozialwissenschaften, 2005.
- Schlüssel-Labor für Big Data Strategie: „Blockdaten 5.0: Theorie und Methode der Datensoziologie“, CITIC Verlag, 2019.
- Shi Dan: „Forschung über die Datenrechtszugehörigkeit und den Weg für ihren Schutz im Big Data Zeitalter“, in Journal der Verkehrsuniversität Xi'an, „Sozialwissenschaft“, 3/2018.
- Shi Dan: „Gesetzlicher Schutz und institutioneller Aufbau von Eigentumsrechten für Unternehmensdaten“, in Elektronische Geisteseigentumsrechte, 6/2019.
- Shi Lindong: „Einfache Analyse des Schutzes des persönlichen Datenrechts“, in Journal der Parteischule Fuzhou, 2/2019.
- Shi Pengpeng: „Neue Entwicklung des grundlegenden Rechtsstammbaums und französischen Strafverfahrens – mit der Beeinflussung der Präzedenzfälle von ‚Europäischen Menschenrechtskonvention‘ und ‚Europäischen Menschenrechtsgericht‘ auf das französische Strafverfahren als Zentrum“, in „Journal Jinan“, Philosophie und Sozialwissenschaft, 7/2013.
- Song Jianbao: „Stärkung des juristischen Schutzes von Big Data, um die Umsetzung der nationalen Big-Data-Strategie sicherzustellen“, in Volksgerichtszeitung, 22. Juli 2019.
- Staatsrat der Volksrepublik China: „Aktionsprogramm für Förderung der Entwicklung von Big Data“, 31. 08. 2015.
- Tang Jiyao: „These über Schutz und Regel des chinesischen Strafrechts für Unternehmensdatenrechte im Zeitalter von Big Data“, in „Journal der Polizeihochschule Shandong“, 3/2019.
- Tong Linjie & Guo Chengcheng: „Weg zur Expansion, Entfremdung und Regelaufstellung der Macht von Big Data“, in „Forschung über Handelswirtschaft“, 4/2019.

- Ulrich Beck, Deng Zhenglai u. Shen Guolin: „Risikogesellschaft und China – Dialog mit dem deutschen Sozialwissenschaftler Ulrich Beck“, in „Forschung über Sozialwissenschaft“, 5/2010.
- Wang Chunye: „Über die Intervention des Privatrechts in Bereich der öffentlichen Macht und Intervention des öffentlichen Rechts in Bereich des privaten Rechts sowie Vervollständigung des verwaltungsrechtswissenschaftlichen Inhalts“, in „Sozialwissenschaft der Inneren Mongolei“, Chinesische Version, 1/2008.
- Wang Haiming: „Grundsatz der Ethik“, Peking University Press, 2009.
- Wang Liming: „Über gesetzlichen Schutz des persönlichen Informationsrechts— mit der Abgrenzung des Privatinformationsrechts vom Recht auf Privatsphäre als Zentrum“, in „Moderne Rechtskunde“, 4/2013.
- Wang Xiuxiu: „Gesetzgebungstheorie über Schutz von personenbezogenen Daten im Hintergrund der Big Data“, Verlag der Zhejiang Universität, 2018.
- Wang Xiuzhe: „Wiederaufbau des Systems zum gesetzlichen Schutz der persönlichen Informationen im Zeitalter von Big Data“, in „Forum der Rechtskunde“, 6/2018.
- Wang Yuan, Huang Daoli u. Yang Songru: „Studie über die Natur und das Eigentum an Datenrechten“, in Informationssicherheit und Kommunikationsschutz, 5/ 2017.
- Wen Yu: „These über Rechtssystem personenbezogener Daten – zugleich zu ‚Rechtslücke der Sesam-Service-Vereinbarung‘“, in „Gansu Sozialwissenschaft“, 2/ 2019.
- Wen Yu: „Über die gesetzliche Eigenschaft der Big Data und Bedeutung der Klassifizierung“, in „Gansu Sozialwissenschaft“, 6/2018.
- Wen Yuheng: „Transformation der Normalform, Begriffswahl und Zugehörigkeitssubjekt der gesetzlichen Festlegung von Datenrechten“, in Journal Nordosten Pädagogische Universität, „Philosophie und Sozialwissenschaften“, 5/2019.
- Wen Yuheng: „Über die privatrechtliche Struktur des Dateneigentumsrechts“, Doktorarbeit; Xiangtan Universität, 2018.
- Wu Weiguang: „Kritik an der Schutztheorie der privaten Rechte personenbezogener Daten unter Big-Data-Technologie“, in Politik und Recht, 7/2016.
- Xi Po: „Die schweigsamen Datenrechte erwachen nun wieder“, in „Zeitung“ Volkskongress der politischen Konsultation, 25. April 2018.
- Xia Yikun: „Versuchsweise Kommentar über Konnotation, Entstehungshintergrund und Hauptfragen der Regierungsdatenregulierung“, 9/2018.
- Xiang Liling u. Gao Qianyun: „Erforschung und Analyse von Merkmalen, grundlegenden Eigenschaften und Inhalten des Rechts auf personenbezogenen Daten im Big Data Zeitalter“, in „Informationstheorie und Ergründung“, 9/2018.
- Yan Lidong: „Erforschung des Rechts auf personenbezogene Daten mit dem Blickwinkel des ‚Rechtsbündels‘“, in „Dongfang Rechtskunde“, 2/2019.

- Yang Weidong: „Effektiv mit den ethischen Fragen der Big-Data-Technologie umgehen“, in Volkszeitung, 23. März 2018.
- Zentrales Büro für Zusammenstellung und Übersetzung Sämtliche Werke von Marx und Engels (Bd. 19). Volksverlag, 1972.
- Zentrales Büro für Zusammenstellung und Übersetzung Sämtliche Werke von Marx und Engels (Bd. 19). Volksverlag, 1963.
- Zhang Endian: „Interpretationsrecht des Algorithmus mitten im Zeitalter von Big Data: Hintergrund, Logik und Struktur“, in Rechtsforum, 4/2019.
- Zhang Jihong: „Dilemma und Lösung der Selbstregulierung des Schutzes personenbezogener Daten durch die Industrie im Zeitalter von Big Data“, in Recht und Wirtschaft, 6/2018.
- Zhang Jinfan: „Tradition und neuzeitliche Transformation der chinesischen Gesetze“, Rechtsverlag, 2009.
- Zhang Linghan: „Der Aufstieg, die Entfremdung und die gesetzliche Regulierung der algorithmischen Macht“, in Studium der Rechtswissenschaften und Wirtschaft“, 4/2019.
- Zhang Suhua u. Li Yanan: „Wahl des Weges zum Datenschutz“, in „Akademiewelt“, 7/2018.
- Zhang Xinbao: „Von Privatsphäre zu Privatinformation: Theorie und Systemanordnung zu Wiederbalancierung der Interessen“, 3/2015.
- Zhang Xinbao: „Studie und Diskussion über den hauptsächlichsten Widerspruch der Gesetzgebung zum Schutzrecht für personenbezogene Informationen in China“, in Journal Jilin Universität, Sozialwissenschaft 5/2018.
- Zhang Yanan: „Teilhabe an Regierungsdaten: innerer Hauptinhalt, rechtsstaatliche Barriere und deren Durchbruchsweg“, in „Theoretische Ergründung“, 5/2019.
- Zhang Yang: „Das Dilemma der Legalisierung der Datenrechte und ihre vertragliche Regulierung“, in Wissenschaft-Technologie und Recht, 6/2016.
- Zheng Ge: „Zwischen dem Ansporn zu Innovation und dem Schutz des Menschenrechts – wie das Gesetz auf die Herausforderung der Neuerung der Big Data Technologie reagieren“, in Erforschung und freie Ansichten, 7/2016.
- Zheng Zhihang: „Gemeinsame Co-Regulierung: gesetzliche und technologische Regulierung in der Cyber-Gesellschaft“, in „Chinesische Rechtskunde“, 2/2018.
- Zhu Lei: „Abklärung des Dateneigentumsrechts durch Gesetzgebung“, Economic Daily, 21. Mai 2019.

Teilhaberechte

Daten sind zu einer Art grundlegender strategischer Ressource des Staats geworden. Wie alle Ressourcen auf der Erde haben Daten auch die klare Eigenschaft der Knappheit. Der Wert von Daten kann jedoch reichlicher werden, wenn sie gemeinsam genutzt werden. Man kann sagen, dass die Teilhabe ein wichtiges Mittel für die Menschheit ist, sich mit dem Problem der Datenknappheit auseinanderzusetzen und den Datenwert zu steigern. Sie ist auch ein unvermeidlicher Trend der Entwicklung der menschlichen Zivilisation und eine Anforderung unserer Zeit. Um die ordnungsgemäße Entwicklung und Teilhabe von Daten zu fördern, haben wir den Begriff der „Teilhaberechte“ vorgeschlagen, um den Wert der Datenteilhabe zu einem Recht aufzuwerten. Das Teilhaberecht, das auf Altruismus beruht, ist das Wesen der Datenrechte. Seine Geburt wird sicherlich die rechtlichen Grundsätze, die soziale Ordnung und die wirtschaftliche Grundlage der Menschheit rekonstruieren.

Abschnitt I Gesetzliche Begründung der Teilhaberechte

Der Aufstieg der Sharing-Wirtschaft lässt Menschen die Teilhabe erneut überdenken. Mit Einsicht in die Entwicklungsgeschichte der menschlichen Zivilisation kann man feststellen, dass sich die Idee der Teilhabe seit Langem schon tief in die Benutzung von Materialien und Daten eindringt und eine grundlegende und normale Methode zur Verwendung von Materialien und Daten ist. Kredit, Transaktion, Teilhabe und Öffnung etc. sind gängige Arten der Teilhabe. Der Wert der Teilhabe hat seit

Langem schon in den Köpfen der Menschen Wurzeln geschlagen und ist zum Teil der Grundwerte der Menschheit geworden. Um den Wert der Teilhabe zu schützen, schlagen wir den Begriff des „Teilhaberechts“ vor, damit der Wert der Teilhabe als Teil des Grundwerts von Daten aufrechterhalten werden kann. Wie das Recht auf Freiheit und Gleichheit ist es eines der Grundrechte der Menschheit.

(I) Von Teilhabe an Dingen zur Teilhabe an Daten

Teilhabe ist seit der Antike ein wesentlicher Bestandteil der Produktion und des Lebens der Menschheit. Dinge werden ausgeliehen, vermietet und gehandelt, Menschen kommunizieren miteinander und Unternehmen arbeiten für gemeinsame Vorteile zusammen usw. All dies kann als Aktivität der Teilhabe angesehen werden. Mit dem Beginn der Ära von Big Data und dem Aufstieg der Sharing-Ökonomie werden öffentliche Daten geöffnet, Geschäftsdaten gehandelt und persönliche Daten geteilt, all dies spielt nach und nach eine immer wichtigere Rolle in wirtschaftlichen und sozialen Aktivitäten und wird zum wichtigsten Mittel, um den Datenwert auszugraben.

1. Entwicklung des Bewusstseins der Teilhabe

Teilhabe ist eines der wichtigen Kennzeichen der menschlichen Zivilisation. In der modernen Sprache bedeutet Teilhabe, Dinge öffentlich zu machen und gemeinsam zu nutzen. Auf Chinesisch tauchte das Wort erstmals in „Chronik von verschiedenen Ländern im Königreich von östlichen Zhou“ auf: „Herzog Jing von Qi genießt nicht nur alleine das Glück und ist bereit gemeinsam zu teilen.“ Das zeigte die Präferenz der Menschheit für Teilhabe. In der „Vermittlung von Riten des Buches der Riten“ gab es die frühen Konzepte wie „die ganzen Welt als eine Gemeinschaft“ und die „Gesellschaft von großer Harmonie“, die auch viel mit dem Bewusstsein der gemeinsamen Teilhabe zu tun haben und diese Präferenz und Begriffe zeigten auch die Idee und Gedanken der menschlichen Teilhabe. In der Zwischenzeit ist das Bewusstsein für

Teilhabe auch im antiken Griechenland zu finden. Zum Beispiel gab es das Konzept einer politischen Gemeinschaft, die gemeinsame Ziele, Interessen und Werte usw. hatte, wie sie von Bürgern desselben Stadtstaates geteilt wurden. Mit dem Aufstieg der industriellen Produktion in großem Maßstab und der modernen Rationalität der Aufklärung änderte sich das Paradigma der Teilhabe jedoch allmählich. Mit dem Hinausgehen über rein moralischer Teilhabe wie universeller Liebe, Harmonie und Fairness usw. betonte sie vielmehr Gesellschaftsvertrag und Rationalitätswert. So ist die Teilhabe zu einer rationalen Norm für Lösung von Problemen in persönlichen und sozialen Beziehungen geworden (Liu Ling 2019). Vor dem Aufstieg der Sharing-Wirtschaft wurde der Wert der Teilhabe jedoch lange ignoriert. Die Sharing-Wirtschaft entstand aus dem Begriff „koordinierten Konsum“, der von Marcus Felson und Joel Spaeth, amerikanischen Soziologieprofessoren 1978 erstmals vorgeschlagen wurde. Der „koordinierte Konsum“ gilt als Ereignis, „bei de[m] eine oder mehrere Personen im Rahmen gemeinsamer Aktivitäten mit einer oder mehreren anderen wirtschaftliche Erzeugnisse oder Dienstleistungen konsumieren.“ Später stellte Martin L. Weitzman 1984 das Konzept der „Sharing Economy“ in seinem Buch „The Sharing Economy: Conquering Stagflation“ vor, bei dem es hauptsächlich darum ging, wie die Unternehmenseinnahmen zwischen Arbeitern und Kapitalisten zu teilen. Der Autor legte den Schwerpunkt auf die Gewinnverteilung auf Mikroebene und schlug vor, ein neues Gewinnteilhabesystem sowie eine Finanz- und Steuerpolitik einzuführen, um das Problem der Koexistenz der Inflation und Stagflation in der wirtschaftlichen Entwicklung im Westen anzugehen. Im Jahre 2010 haben Rachel Botsman und Roo Rogers die Sharing Economy zum ersten Mal in seinem Buch „What’s Mine is Yours“ die Form der Sharing-Wirtschaft definiert und erläutert. Ihnen zufolge „ist das ein neues Muster von Konsum und Leben“. Da die auf Idee der Teilhabe basierten Unternehmen wie Uber, Airbnb und DiDi etc. schnell wachsen und jeden Aspekt der Produktion und des Lebens der Menschheit durchdringen, hat man begonnen, den Wert der Teilhabe erneut zu überdenken. Bisher hat die Teilhabe die Grenze eines einzelnen Unternehmens überschritten, in die Gesellschaft außerhalb des

Unternehmens ausgeweitet und dann die Beziehungen des Eigentumsrechts durchgebrochen, sodass man an alle Ressourcen teilhaben kann.

2. Ergründende Analyse der Arten der Teilhabe

Das frühe Bewusstsein für Teilhabe derivierte verschiedene Arten der Teilhabe: Arbeitsteilung und Zusammenarbeit, verbale Kommunikation, schriftliche Aufzeichnung, Warenhandel, Datenaustausch und so weiter. Diese gebräuchlichen Arten der Teilhabe sind eine wichtige Kraft, die die Entwicklung der menschlichen Zivilisation fördert. Objekte, die teilbar sind, sind entweder greifbare Dinge oder Daten. Die Teilhabe von materiellen Dingen gehört zur physischen Welt, während die Teilhabe an Daten, die immateriell sind, zur virtuellen Welt gehört. Sprachen, Schriften, Daten und Informationen etc. können alle in der Kategorie der Datenteilhabe erfasst werden.

In der früheren Antike mussten die Menschen zusammenschließen und ihre Fähigkeiten teilhaben, um die Herausforderungen der Natur zu bewältigen. Einige waren für Eintopfen und Netz-Stricken verantwortlich, einige für Sammeln wilder Früchte und andere für Jagd usw., was ihre Produktivität und Überlebensfähigkeit erheblich verbesserte. So wurde das Überleben der Menschheit gesichert. In verschiedenen primitiven Herdenstämmen, die allmählich entstanden, blühten die Menschen auf und machten ihren ersten Schritt und bildeten eine solide Grundlage dafür, um der Herr der Erde zu sein. Man kann daher mit Recht sagen, dass die Arbeitsteilung und Zusammenarbeit als ein wichtiger Bestandteil der Teilhabe, was die Menschheit praktizierte, ist, sie ist sowohl eine Wahl der natürlichen Umgebung als auch das, was für die menschliche Entwicklung erforderlich war. Sprache ist ein Kommunikationsmittel, während Kommunikation eine Art der Teilhabe ist. Was den Ursprung der Sprache betrifft, ist eine wichtige Frage, die die akademische Welt bis jetzt immer noch nicht völlig gelöst hat und es gibt immer noch mehrere Streitigkeiten. Wir sind der Meinung, dass die Sprache ein Produkt des menschlichen Kampfes gegen die Natur ist. Im Prozess der Zusammenarbeit brauchte die Menschheit Kommunikation, während gestische Handbewegungen angesichts der rauen natürlichen Bedingungen bei Weitem nicht genug waren.

Die gesprochene Sprache wurde daher dringend benötigt, um die Effizienz der Zusammenarbeit und Kommunikation zu steigern. Mit Sprache kann man ihre Gedanken und Ideen mit anderen teilen, auf andere Ausdrucksweise kommunizieren und ihre Produktivität erheblich erhöhen. Die Sprache ist auch heute noch eine hauptsächliche Ausdrucksweise für die Kommunikation der Menschheit, und nichts anderes kann sie völlig ersetzen. Die Schriftzeichen, die aus alten Wandgemälden geboren wurden, sind ein weiteres Werkzeug der Teilhabe, das für Menschen einzigartig ist. Archaische Menschen schnitzten Muster an Höhlenwänden, um Heldentat aufzuzeichnen. Aber diese verworrene Methode wurde später bei Weitem nicht mehr ausreichend, um die Bedürfnisse der menschlichen Entwicklung zu befriedigen. Schließlich entwickelte sich das Muster an den Höhlenwänden zu dingartigen Schriftzeichen—Bilderschriften, Hieroglyphen und Keilschriften usw., die sich heute in verschiedene Schriftsysteme verwandeln. Die Entstehung von Schriftsystemen ist ein großes Ereignis in der Geschichte der menschlichen Zivilisation. Sie tragen die Erfahrungen des Überlebens, Erfolge der Entwicklung und das gesammelte Wissen der Menschheit usw. mit einzigartiger Faszination voran, sodass sie mit anderen und Nachkömmlingen geteilt werden können und die menschliche Zivilisation kontinuierlich vorantreiben können. Sprache und Schrift sind beide Medien der Teilhabe, aber sie unterscheiden sich stark voneinander. Die Sprache konzentriert sich auf Teilhabe an Informationen, während die Schriften Informationen und Wissen tragen. Sowohl der Informationsaustausch als auch die Weiterreichung von Wissen waren frühe Aktivitäten der Teilhabe in der Geschichte der Menschheit. Der Beitrag von Sprache und Schrift zur Menschheit ist grundlegend und revolutionär und hilft der Menschheit, sich inmitten von Evolution und Wettbewerb von allen Arten der Dinge abzuheben und schließlich der Herr der Erde zu werden (Schlüssel-Labor von Big-Data-Strategie 2019, S. 188).

Warentransaktionen sind eines der wichtigsten Merkmale der modernen Gesellschaft und auch eine wichtige Art der Teilhabe. Vom anfänglichen Tauschhandel über die Entstehung von Geld bis hin zur Entstehung wirtschaftlicher Theorien wächst und expandiert die Warentransaktion ständig und ist zu einer unverzichtbaren sozialen und wirtschaftlichen Aktivität in der menschlichen Gesellschaft geworden. Die Teilhabe kann

in entgeltliche Teilhabe und unentgeltliche Teilhabe unterteilt werden, während die Warentransaktion im Allgemeinen zur Ersteren gehört. Durch eine Warentransaktion teilt man das, was er/sie besitzt, mit anderen und erhält dafür bestimmtes Entgelt. Dies erhöht die Motivation zur Teilhabe, erzielt Gewinn-Gewinn-Ergebnisse für beide Seiten der Transaktion und löst das Problem der Warenknappheit. Mit dem Beginn der Ära von Big Data sind Daten als ein wichtiges Produktionsmittel auch in den Bereich der Teilhabe aufgenommen. Aufgrund der Trägheit der geschichtlichen Entwicklung und des Mangels an Planung auf höchster Ebene haben sich jedoch viele „Dateninseln“ gebildet und Datenressourcen werden nicht effektiv genutzt. Da Daten von Natur aus relationale Eigenschaft haben, kann der Wert von Daten nur dann voll zur Geltung gebracht werden, wenn „Dateninseln“ beseitigt werden und Daten besser verbunden werden. Die Teilhabe dient als ein wichtiges Mittel zur Beseitigung von „Dateninseln“. Es gibt hauptsächlich zwei Methoden für die Teilhabe von Daten: offener Zugriff auf Daten und Datentransaktionen. Beide befinden sich jetzt noch in einem frühen Entwicklungsstadium und haben viele Probleme zu lösen. Als der wichtigste Motor der Big-Data-Entwicklung bietet die Datenteilhabe jedoch viel Raum für die weiteren Entwicklungen.

3. Wertimplikation der Teilhabe

In der Geschichte der Menschheit hat jeder Sprung der Produktivkräfte die menschliche Zivilisation mit großen Schritten vorangebracht. Die Teilhabe konzentriert sich auf Maximierung der öffentlichen Interessen, treibt tief greifende Veränderungen in der Produktions- und Lebensweise der Menschheit voran, fördert die Produktivität und den Lebensstandard der Menschheit erheblich und bringt neue Paradigmen hervor, die die Entwicklung der menschlichen Zivilisation vorantreiben. Wie wir sehen können, hat die Teilhabe Auswirkungen auf Subjekt, Objekt und Inhalt in unterschiedlichem Grad. Daher spielt die Teilhabe eine einzigartige Rolle bei der Reaktion auf die Bedürfnisse der wirtschaftlichen und sozialen Entwicklung der Menschheit. Für das Subjekt ist die Abdeckung der Teilhabe weit und breit. Sie kann Unterschiede und Diskriminierung in jeglicher Form und Denkweise überbrücken und auf dieser Grundlage

beseitigen. Jeder kann das Subjekt der Teilhabe sein. Für das Objekt der Teilhabe können alle Errungenschaften der menschlichen Zivilisation gemeinsam genutzt werden. In Bezug auf den Inhalt der Teilhabe können Fortschritte in allen Aspekten der menschlichen Zivilisation einbezogen werden. Mit diesen Merkmalen hat die Teilhabe einen realistischen Weg für die wirtschaftliche und soziale Entwicklung der Menschheit angeboten, den grundlegenden Anforderungen der wirtschaftlichen und sozialen Entwicklung der menschlichen Gesellschaft entsprochen und positive Erwartungen für das Anstreben der Menschheit nach einem besseren Leben und Fortschritten in der Zivilisation geliefert. Teilhabe ist eine wichtige Triebkraft für das Überleben und Entwicklung der Menschheit, da sie die kollektive Kraft der Menschen stärken, die Natur effektiv nutzen und transformieren, die menschliche Kommunikation fördern und die synergetische Zusammenarbeit effizienter erhöhen kann. Sie kann auch die Weisheit an zukünftige Generationen weiter fortsetzen, um den menschlichen Fortschritt zu fördern; sie kann kommerzielle Aktivitäten vorantreiben, das Problem der Ressourcenknappheit lösen; sie kann auch den digitalen Raum schaffen, um die Menschheit in eine neue Ära der digitalen Zivilisation zu bringen. Ob in der Vergangenheit, jetzt oder künftig ist und bleibt die Teilhabe für das gemeinsame Leben der Menschheit von unermesslicher Bedeutung.

(II) Vom Mehrwert zum Teilhabewert

Der Marxismus ist der Ansicht, dass die widersprüchlichen Wechselwirkungen zwischen Produktivkräften und Produktionsverhältnissen sowie zwischen wirtschaftlicher Basis und Überbau als grundlegende Triebkraft dienen, die die menschliche Gesellschaft von einer niedrigen auf eine höhere Ebene treibt. Seit dem Beginn der kapitalistischen Geschichte wurden größere soziale Produktivkräfte als je zuvor geschaffen und die menschliche Gesellschaft hat großen Fortschritt gemacht. Nach der Logik des Kapitals dienen die technische Revolution, die industrielle Transformation, die politische Revolution und die philosophische Revolution usw. alle jedoch nur der Kapitalaufwertung. Das hat dazu geführt, dass

sich die Kapitalisten immer mehr bemühen, um den Mehrwert immer verrückter auszuplündern und zu kontrollieren, sodass die Menschen auf dem Weg der Entfremdung immer weiter gehen (Hu Shouyong 2018). Die Theorie des Mehrwerts verliert dann allmählich ihre Erklärungsfähigkeit und die Theorie des Wertes der Teilhabe taucht im richtigen Moment auf.

1. Entwicklung der Werttheorien

Als eine wichtige Kategorie von Theorien in der Ökonomie gehen Werttheorien auf die Zeit zurück, als die Ware entstand. Ein Ding kann deshalb zu Ware werden, weil der Wert des Dinges in der Ware kondensiert hat. Ein wertloses Gut kann kaum zur Ware werden. Basierend auf Erben der Gedanken seiner Vorgänger, insbesondere wie Weise Sokrates und Platon, schuf Aristoteles eine relativ vollständige Reihe von Wertgedanken, aus denen verschiedene Werttheorien hervorgehen. Etwa 2000 Jahre lang seither hatten Aristoteles' Gedanken über den Wert jedoch keine große Chance, in der Praxis bewiesen und weiterentwickelt zu werden, und daher nahm keine Werttheorie wirklich Gestalt an.

In einer „Untersuchung über das Wesen und die Ursachen des Volkswohlstandes“ schuf Adam Smith ein vollständiges System der politischen Ökonomie. Ihm zufolge bestimmt die Menge an Arbeit, die es kostet, eine Ware herzustellen, den Wert der Ware; oder mit anderen Worten, der Wert einer Ware entspricht der Arbeitsmenge, die er kaufen kann. Deshalb bestimmt der Wert den Austauschwert. Während die Arbeitsmenge das einzige richtige Maß für den Tauschwert und Wert ist, wurde der Preis in drei Arten von Einnahmen wie Lohn, Gewinn und Pachtzins zersetzt (Guan Dehua & Kong Xiaohong 2013, S. 8). Die Forschungsergebnisse von Adam Smith bilden eine solide Grundlage für zukünftige Wertstudien. Smiths Theorie hat jedoch ihre Mängel: Es fehlt an Ausarbeitung von Arbeitskräften und Produktionspreisen und das Verhältnis zwischen Wertschöpfung und Wertverteilung wurde verwechselt. Infolgedessen entstanden daraus drei große Schulen unterschiedlicher Werttheorien.

Die von David Ricardo und Karl Marx vertretene Schule der Theorie des Arbeitswerts: Diese Schule legte Wert darauf, den Wert aus Sicht der

Angebotsseite zu analysieren. David Ricardo korrigierte das Argument von Adam Smith, dass „eine Ware ohne Gebrauchswert auch einen Tauschwert besitzt“, er meinte, „dieser Wert soll durch die verbrauchte aber nicht die gekaufte Arbeit bestimmt werden“. Das machte Ricardo zu dem, der die Arbeitswerttheorie schließlich und endlich vervollständigte. Mit steigender Produktivität entstand jedoch ein relativer Warenüberschuss, und der Wert vieler Waren konnte auf dem Markt nicht realisiert werden, demzufolge löste sich Ricardos Werttheorie selbst aus. Basierend auf Ricardos Theorie schlug Karl Marx die Theorie über Dualität von Ware und Dualität der Arbeit vor. Er teilte die Arbeit in konkrete Arbeit, die Gebrauchswert schafft und abstrakte Arbeit, die Wert schafft. Anschließend schlug er die Theorie des Mehrwerts vor und schlussfolgerte die Umrechnung vom Wert zum Produktionspreis (Meng Kui 2013). Die Werttheorie von Marx spiegelte die tief greifenden sozialen Beziehungen zwischen den Menschen hinter dem Warenaustausch wider und nagelte sie als Beziehungen zwischen Menschen fest. Das ist der grundlegende Unterschied zwischen seiner und Ricardos Arbeitswerttheorie.

Die Schule der Grenzwerttheorie, vertreten durch Carl Menger, William Jevons, Leon Walras und John Bates Clark befürwortete den Nachfragedeterminismus und definierte den Wert als Grenznutzen basierend auf subjektiver Bewertung.¹ Diese Schule geht davon aus, dass der durch Änderung der Verbrauchsmenge verursachte Änderung des Nutzens der Grenznutzen ist, d.h. der Wert wird durch den Grenznutzen einer Ware bestimmt. Sie schlug die Theorie der Grenzproduktivität vor, die die Objektivität der Werts substanz untergräbt und die Arbeitswerttheorie gründlich leugnet. Da die Grenzwerttheorie besonderes Gewicht auf Studie zum Verbrauchsbereich legte und sich auf Konsum und Verteilung im Konsumbereich konzentrierte, veranschaulichte sie systematisch das Konsumentengleichgewicht (Gleichgewicht des Austauschs) und das

1 Der Grenznutzen bezieht sich auf den erhöhten Zufriedenheitsgrad durch den Verbrauch einer zusätzlichen Einheit bestimmten Materials. Die Bedeutung von Margin ist Inkrement, das sich auf das Inkrement der abhängigen Variablen bezieht, das durch die Zunahme der unabhängigen Variablen verursacht wird. Im Grenznutzen ist die unabhängige Variable der Materialverbrauch, während die funktionale Variable der Zufriedenheitsgrad oder Nutzen ist.

Produzentengleichgewicht (Gleichgewicht von Arbeits- und Kapitaleinsatz) und stellte den Konsumbereich, der in der wirtschaftlichen Forschung nicht genug beachtet wurde, in den Mittelpunkt und legte Grundstein für Gründung des mikroökonomischen Forschungssystems, sodass sie zum Ursprung der modernen westlichen Ökonomie geworden ist (Guan Dehua & Kong Xiaohong 2013, S. 99–102).

Die Schule der Wertgleichgewichtstheorie, vertreten durch Alfred Marshall und Paul Samuelson: Diese Schule teilte die Überzeugung, dass weder Angebot noch Nachfrage bei der Bestimmung des Wertes einer Ware vernachlässigt werden können. Der Wert der Ware wird durch die Marktkräfte bestimmt, d.h. durch das Gleichgewicht von Angebot und Nachfrage, nicht nur durch Produktion oder Verbrauch alleine. Daraus ist ersichtlich, dass die Theorie des Wertgleichgewichts eine Kombination der beiden oben genannten Theorien (Arbeitswerttheorie und Grenzwerttheorie) ist. Sie spiegelt die Beziehungen zwischen Menschen und Dingen wider, nämlich die Beziehung zwischen bestimmten Gütern und den Bedürfnissen der gesamten Gesellschaft, oder allgemeiner gesagt, die Beziehungen zwischen Mensch und Natur. Mit dem Nutzenmaß² spiegelt sie die Beziehungen zwischen dem Bedarfsgrad der Menschen und dem Knappheitsgrad der Dinge oder der Schwierigkeitsgrad, ein bestimmtes Ding zu erhalten wider. Dies hat heute eine starke Erklärungskraft für viele wirtschaftliche Phänomene (Meng Kui 2013). Daher ist die Theorie des Wertgleichgewichts in der westlichen Wirtschaft stets vorherrschend, seit sie von Marshall vorgeschlagen wurde.

Nachdem Marshall die Theorie des Wertgleichgewichts gegründet hatte, wurde bisher kein wirklicher Durchbruch auf dem Gebiet der Werttheorie erzielt. Insbesondere seit der Geburt des Internets sind Trends der Globalisierung, Vernetzung, Informatisierung und Virtualisierung heutzutage immer klar, aber keine der drei wichtigsten Werttheorien kann eine überzeugende Interpretation für anhaltende wirtschaftliche Phänomene liefern oder Leitlinien für moderne wirtschaftliche Operationen bieten.

2 Bei Nutzenmaß wird hauptsächlich der Kostenunterschied zwischen den durch Erfüllung sozialer Nachfrage entstandenen Nutzen und den zur Befriedigung der sozialen Anforderungen ausgegebenen Kosten berechnet.

Viele aufstrebende ökonomische Theorien wie Informationsökonomie, öffentliche Ökonomie, Spieltheorie, neue institutionelle Ökonomie und psychologische Ökonomie etc. haben ihre neue Werttheorien vorgeschlagen, aber sie sind lediglich eine Entwicklung und Ergänzung zu den drei hier erläuterten Hauptwerttheorien, sie können keine systematische und organische Ganzheit bilden und haben auch keine universelle Anwendbarkeit. Deshalb braucht die Entwicklung der Wirtschaft und Gesellschaft jetzt neue Werttheorien.

2. Vom Mehrwert zum Teilhabewert

Aus Sicht der Form der Wirtschaft und Gesellschaft gibt es in der heutigen Welt Kapitalismus und Sozialismus. Die von Marx und Engels vorgeschlagene Mehrwerttheorie ist eine Theorie, die den kapitalistischen Produktionsprozess analysiert. In Bezug auf Mehrwert haben sie so ausgedrückt: „Der Mehrwert bezieht sich auf den Restbetrag, der vom Warenwert abzüglich des Wertes der verbrauchten produktbildenden Elemente, d.h. der Produktions- und Arbeitsmittel übrig bleibt“ (Central Compilation and Translation Bureau 1972, S. 235). Zusammenfassend haben sie den kapitalistischen Produktionsprozess als Ganzes als den Produktionsprozess des Mehrwerts bezeichnet. Im Produktionsbereich wird der Mehrwert in Form von Waren erzeugt, während der Mehrwert im Umlauf durch Verkauf von Waren realisiert wird. Daher bildet sich ein scharfer Widerspruch zwischen der Produktion und der Realisierung des Mehrwerts: Der Produzent würde im Prozess der Warenproduktion so viel Mehrwert wie möglich in Besitz nehmen, um mehr Gewinn zu erzielen, während in der Zwischenzeit eine hohe Mehrwertrate unweigerlich die Realisierung von Mehrwert der Waren im Umlauf behindert, weshalb eine Wirtschaftskrise eintritt (Meng Kui 2013). Die Theorie des Mehrwerts von Max und Engels enthüllte die grundlegendste Regelmäßigkeit des Betriebs der kapitalistischen Wirtschaft, die wirtschaftliche Wurzel des Antagonismus zwischen Bourgeoisie und Proletariat und den fundamentalen Grund, warum der Kapitalismus zwangsläufig sterben muss. Die Theorie des Mehrwerts kann die wesentlichen Merkmale der Gesellschaft der sozialistischen Wirtschaft jedoch nicht widerspiegeln, und

dafür steht derzeit auch keine Werttheorie zur Verfügung, die die sozialistische Wirtschaft perfekt interpretieren kann. Unter diesen Umständen hat der Wert der Teilhabe mit dem Aufstieg der Teilhabewirtschaft erneut zunehmende Aufmerksamkeit erregt, und die Theorie über Teilhabewert zeichnet sich dadurch aus, dass sie das Wertgesetz des Sozialismus und sogar der ganzen Gesellschaft völlig neu interpretiert hat.

Die sogenannte Theorie über Teilhabewert ist eine Theorie, die sich um den Wert dreht, der durch Aktivität der Teilhabe geschaffen wird, zustande gekommen hat. Da die Ressourcen auf der Erde knapp sind, sind sie alle auf der Erde nützlich und müssen voll ausgeschöpft werden. Mittlerweile haben wir nur diese eine Erde, die wir alle teilen, und jeder hat das gleiche Recht, seine Ressourcen gut und effektiv zu nutzen (Schlüssel-Labor von Big-Data-Strategie 2019, S. 194). Dies erfordert, dass wir die Effizienz der Ressourcennutzung durch Teilhabe steigern. Das ist die Quelle und Notwendigkeit, wo und warum der Wert der Teilhabe entsteht. Während des Wertschöpfungsprozesses spielen die Anbieter der drei Produktionsfaktoren Arbeit, Kapital und Land ihre Rolle. Sie haben direkt oder indirekt daran teilgehabt und sollen natürlich an der Wertverteilung teilnehmen. Deshalb kann die Teilhabe Wert schaffen. Wie die Theorie des Mehrwerts basiert auch die Theorie des Teilhabewerts auf der Arbeitswerttheorie. Die Theorie über Teilhabewert, ob in einer kapitalistischen oder sozialistischen Gesellschaft, befürwortet, dass Arbeitende den Wert genießen können sollen, den sie schaffen. Dies kombiniert die Verteilung nach Arbeit und die Verteilung nach Produktionsfaktoren, legt die theoretische Grundlage für die Einkommensverteilung in der Gesellschaft, bringt alle Mitglieder der Gesellschaft in eine Gemeinschaft gemeinsamer Interessen, setzt die Begeisterung aller Seiten für die Produktion frei und emanzipiert und entwickelt weiter die Produktivkräfte.

3. Schöpfung des Werts der Teilhabe

Mit der Entwicklung des Zeitalters wächst der Einfluss der Teilhabe auf der ganzen Welt und der Wert der Teilhabe steigt auch entsprechend. Erstens senkt der Aufstieg der neuen Generation von Informationstechnologien wie Internet, Big Data und künstlicher Intelligenz die Kosten

für Teilhabe, und die Plattformen der Teilhabe erhöhen die Effizienz der Abstimmung von Angebot und Nachfrage erheblich, senken die Grenzkosten für Teilhabeobjekt auf nahezu null und so erweitern den Umfang der Teilhabe. Zweitens findet die Teilhabe eine solide Ressourcengrundlage, da die materiellen und kulturellen Ressourcen insgesamt an Quantität zunehmen: Einerseits ist es nicht mehr das ultimative Ziel, Dinge in den eigenen Besitz zu bringen, und die Menschen sind eher bereit, ihre Dinge gemeinsam mit anderen teilzuhaben und liefern damit die Ressourcenbasis für Wertschöpfung der Teilhabe; andererseits bieten Unterschiede in der Konsumkraft zwischen verschiedenen Schichten der Gesellschaft Bedingungen für den Ressourcenfluss. Schließlich haben die Menschen ihre Gedanken für Produktion und Leben jetzt geändert, das Bewusstsein der ganzen Gesellschaft für die Teilhabewirtschaft wird ständig erwacht und sublimiert. Sie sind bereit, Ressourcen durch Teilhabe neu zuzuweisen. Dies erhöht die Effizienz der Ressourcennutzung erheblich, verringert die Überproduktion der Waren und Ressourcen und die Abhängigkeit von außen. So wird Teilhabewert geschaffen (Liu Genrong 2017).

Teilhabe ist sowohl ein Wirtschaftsmodell als auch ein Sozialmodell, deren Wert sich hauptsächlich in den folgenden drei Aspekten widerspiegelt: Erstens bietet sie mehr Initiative, Sicherheit und Transparenz. Im traditionellen Wirtschaftsmodell fehlt dem Markt die Transparenz. In Bezug auf die Qualität der Waren und Dienstleistungen gibt es sehr große Unsicherheiten, und die Verbraucher haben keine Initiative für ihre Verbrauchsentscheidungen. Die Teilhabewirtschaft bietet Verbrauchern aber einen besseren Zugang zu Informationen, damit wird die Transparenz der Waren und Dienstleistungen erhöht und die Verbrauchssicherheit wird wiederum gewährleistet. Zweitens wird die Vertrauenskrise zwischen beiden Seiten der Teilhabe beseitigt. Sowohl bei Warentransaktionen als auch beim Informationsaustausch führt die Informationsasymmetrie zu einem natürlichen Misstrauen zwischen beiden Beteiligten, und sowohl die Warentransaktionen als auch der Informationsaustausch können behindert werden. Im Gegensatz dazu fördert die Teilhabe das Vertrauen zwischen beiden Seiten, da sie während des gesamten Prozesses gut sichtbar ist. Drittens verbessert die Teilhabe das Wohlbefinden beider Seiten. Durch Teilhabe erzielen die

Anbieter Gewinne mit ihrer Bereitstellung von Produkten oder Dienstleistungen, während Verbraucher Produkte und Dienstleistungen, die sie benötigen, durch Teilhabe zu einem niedrigeren Preis erhalten können. Dadurch kann das Wohlbefinden beider Seiten verbessert werden.

Wenn wir untersuchen, wie der Wert der Teilhabe geschaffen wird, stellen wir fest, dass er mindestens die folgenden Faktoren enthält: Erstens müssen regsame Aktivitäten der Teilhabe vorhanden sein. Nur die Aktivität der Teilhabe kann Teilhabewert schaffen. Das ist die Quelle der Produktion des Teilhabewertes. Im Modell der Teilhabe kann man daran teilhaben, solange er über Ressourcen verfügt. Jede Person oder Organisation kann das Subjekt der Teilhabe sein; jede Ware oder Dienstleistung, ob materiell oder immateriell, kann Objekt der Teilhabe werden, solange sie Wert hat und benötigte Waren oder Daten sind. Zweitens muss eine Plattform zur Teilhabe vorhanden sein. Die Teilhabe ist nur möglich, wenn eine Plattform dafür vorhanden ist. Das ist die Grundlage für die Wertschöpfung durch Teilhabe. Während dieses Prozesses fungiert die Plattform hauptsächlich als Vermittler, der Informationen über Angebot und Nachfrage übermittelt und Übereinstimmung von Angebot und Nachfrage usw. bereitzustellen. Da die zu teilhabenden Ressourcen in der Gesellschaft verstreut sind, ist es notwendig, eine Plattform zu haben, auf der sie zusammenkommen, zusammengestellt und ausgestellt werden, Verbindungen zwischen ihnen hergestellt und Geschäfte abgeschlossen werden können, auch potenzielle Anbieter und Bedarfsträger zusammenkommen, damit Ressourcen der Teilhabe trotz zeitlicher und räumlicher Entfernungen miteinander verbunden werden können. Drittens ist die Teilhabe an Nutzungsrecht auf Ressourcen. Das ist die Hauptmotivation für die Wertschöpfung durch Teilhabe. Im traditionellen Modell muss man zuerst das Eigentumsrecht erlangen und dann erhält er das Nutzungsrecht, wenn man diese Ware benutzen will. Dadurch werden viele Ressourcen verschwendet. Die Teilhabe trennt das Eigentumsrecht und das Nutzungsrecht und bildet ein Modell, in dem „Menschen versuchen, Dinge nicht zu besitzen, sondern nur zu nutzen“. So wird die Teilhabe an Nutzungsrecht verwirklicht. Viertens muss es einen soliden Vertrauensmechanismus geben, der als Bindung für Schaffung des Teilhabewertes dient. Die Teilhabe findet hauptsächlich zwischen Fremden statt. Daher ist es notwendig, ein solides und zuverlässiges Vertrauenssystem

zu errichten, um die Frage des Vertrauens zwischen den Fremden zu lösen. Das ist eine wichtige Garantie für die Aktivität der Teilhabe. Fünftens soll ein offenes System für Teilhabe vorhanden sein, was die Garantie für Vitalität der Schöpfung des Teilhabewerts darstellt. Dieses offene Teilhabesystem muss eine niedrige Schwelle für Teilhabe haben, nicht aber im Gegenteil eine Schranke für Zugang. Andernfalls würde der Umfang der Teilhabe kleiner, wenn Subjekte der Teilhabe ausgeschlossen und Ressourcen für Teilhabe erschöpft werden, sodass die Teilhabe ihren Schwung verlieren würde. Nur die Offenheit kann sicherstellen, dass die Teilhabe ihre Größe schnell und kostengünstig erweitern und mehr Teilhabewert schaffen kann (Liu Genrong 2017).

(III) Recht auf Freiheit, Recht auf Gleichheit und Recht auf Teilhabe

Kann die Teilhabe ein Recht sein? Das ist eine Frage, die diskussionswert ist. Die in Deutschland erstmals entstandene Theorie über Teilhaberecht hat sich nach radikalen Veränderungen in verschiedenen Epochen zu einem vergleichsweise ausgereiften theoretischen System entwickelt.

1. Teilhaberecht als Ersatz für das Freiheitsrecht

Als Ersatz für das Recht auf Freiheit zielt das Teilhaberecht hauptsächlich darauf ab, die zentrale Position des Freiheitsrechts im bestehenden Rechtsportfolio einzunehmen. Das ist die wichtige Ansicht von Ernst Forsthoff, ein deutscher Verwaltungsjurist. Die Diskussion über „Teilhaberecht“ im Artikel III in seinem berühmten Werk „Verwaltung als Dienstleister“³ in 1938 gilt tatsächlich als Ursprung der Theorie über Teilhaberecht und

3 Chen Xinmin, ein Gelehrter aus Taiwan, China, veröffentlichte seine Übersetzung des Hauptteils dieses Artikels im dritten Abschnitt „Das ursprüngliche Erscheinungsbild der Konzepte von Leistungsverwaltung und Daseinsvorsorge – Diskussion über die „Verwaltung als Dienstleister“ von Forsthoff in seinem Arbeits-Essays on Public Law. Weitere Informationen zu Forsthoffs Theorie der Teilhaberechte finden Sie unter Chen Xinmin. 2010. Aufsätze zum öffentlichen Recht, Law Press China, S. 39–80.

hat weitreichenden Einfluss gehabt. Forsthoff meinte, dass das Teilhaberecht als Ersatz für das Freiheitsrecht auf Änderungen im Lebensstil der Menschen zurückzuführen ist und eine Abkehr von der Idee des liberalen Rechtsstaats darstellt. Im Zeitalter des liberalen Rechtsstaates zielte die Verwaltungsrechtsprechung darauf ab, das Freiheitsrecht der Einzelnen zu schützen. Da die Daseinsvorsorge jedoch Vorrang vor anderen Aufgaben des Staates hatte, nahm die Bedeutung des Freiheitsrechts der Einzelnen allmählich ab. Daher muss eine faire Gesellschaftsordnung geschaffen werden, und es sollte sichergestellt werden, dass Einzelpersonen an diese Ordnung teilhaben können. Das ist der Hauptgrund, warum Forsthoff die Grundsätze der Verwaltungsrechtskunde aktualisiert hat. Um eine faire Gesellschaftsordnung zu schaffen, muss man auf das Freiheitsrecht verzichten und sich dem Teilhaberecht zuwenden. Das traditionelle Freiheitsrecht ist nicht unbedingt wirtschaftlich, während das Teilhaberecht als Ersatz für Freiheitsrecht wirtschaftlicher, fairer und öffentlicher Natur ist. Durch Einführung der Konzepte von „Daseinsvorsorge“ und „Teilhaberecht“ erweiterte Forsthoff den Geltungsbereich des Verwaltungsrechts und der Verwaltungsrechtskunde erheblich und wurde daher als Vater der Theorie „Leistungsverwaltung“ geehrt. Forsthoffs Forschung zu den Teilhaberechten als Ersatz des Freiheitsrechts hatte weitreichenden Einfluss. Er hatte das Freiheitsrecht von der alleinigen zentralen Position im gesamten Portfolio gestrichen und zu Diskussionen über Teilhaberecht geführt, die bis heute immer noch andauert. Außerdem baute er organische Verbindungen zwischen der Leistungsverwaltung und den Teilhaberechten auf und schloss das Recht auf Teilnahme an öffentlichen Angelegenheiten und das Recht auf soziale Hilfe von der Abdeckung des Teilhaberechts aus. Diese Standpunkte werden heute noch von vielen akzeptiert. Indem Forsthoff das Teilhaberecht als Ersatz für das Freiheitsrecht vorschlug, übertrieb er jedoch die Nachteile des Freiheitsrechts und des liberalen Rechtsstaates nach der industriellen Revolution, übersah das Grundlegende und Stabilität, überbewertete die positiven Aspekte des Teilhaberechts und unterschätzte seine negative Seite. Dies prädestinierte, dass das Konzept der Teilhaberechte als Ersatz für das Freiheitsrecht nur ein Blitz in der Pfanne sein konnte. Wie zu erwarten war, betonte das Grundgesetz der Bundesrepublik Deutschland

nach dem Zweiten Weltkrieg das Freiheitsrecht, was ein klares Zeichen für Ablehnung von Forsthoffs Präferenz für das Teilhaberecht und gleichzeitige Verweigerung des Freiheitsrechts war.

2. Teilhaberecht als Nebenordnung des Freiheitsrechts

In seinen 1959 veröffentlichten „Legal Issues of Service Administration“ gab Forsthoff seinen Vorschlag für Teilhaberecht als Ersatz für das Freiheitsrecht auf und unterschied diese beiden, indem er das Freiheitsrecht als Leitprinzip der intervenierenden Verwaltung und das Teilhaberecht als Leitprinzip der Leistungsverwaltung betrachtete. Da sich Forsthoffs Standpunkt zu Teilhaberecht drastisch geändert hatte, wurde das Teilhaberecht nun dem Freiheitsrecht nebengeordnet. Auch in diesem Buch schlug er die ergänzende Theorie von „Daseinsvorsorge“ vor und argumentierte, dass die Frage der Daseinsvorsorge der Mitglieder der Gesellschaft von der Gesellschaft gelöst werden soll und der Staat seine „ergänzende Funktion“ nur dann ausüben sollte, wenn die Gesellschaft diese Frage ihrer Mitglieder nicht lösen könnte. So bedeutet die „ergänzende Funktion“, dass das Konzept der „Daseinsvorsorge“ nicht mehr initiativ wie zuvor, sondern zu einem passiven Konzept geworden ist. Die Macht von Individuen und Gesellschaft, die zuvor von Forsthoff verunglimpft wurde, gewinnt jetzt wieder Anerkennung und die Abhängigkeit der Individuen vom Staat und den Teilhaberechten wurde auch verringert (Luo Ying 2014). Wenn Forsthoffs Standpunkt zum Teilhaberecht als Ersatz für das Freiheitsrecht die Verachtung des Rechts auf Freiheit und eine „revolutionäre“ Denkweise widerspiegelte, dann zeigte die Nebeneinanderordnung des Teilhaberechts mit dem Freiheitsrecht seinen Respekt vor dem Freiheitsrecht und seine „reformistische“ Denkweise. Mit der Entwicklung der Gesellschaft haben sich die Lebensbedingungen, der Lebensstil und die Bedürfnisse der Menschheit geändert, und ihre Interessen sind auch diversifiziert. Unsere Menschenrechtsgesetzgebung muss auch auf solche Änderungen reagieren. Menschenrechte sind kein starres oder geschlossenes Portfolio, und das Freiheitsrecht ist auch nicht alles von Menschenrechten. Die nach der industriellen Revolution entstandenen Teilhaberechte sollen im System der Menschenrechte einen Platz

haben. Forsthoff sah und akzeptierte die Entstehung und Entwicklung der Dienstverwaltung und schlug die Theorie über das Teilhaberecht als Beiordnung des Freiheitsrechts vor, wobei er beide jeweils als Leitprinzipien der Dienstverwaltung und der Interventionsverwaltung ansah. Dies trug zur Verbesserung der Theorie der Dienstverwaltung bei und hatte großen Einfluss auf die moderne Verwaltungsrechtskunde. Bei dem solchen Einfluss geht es jedoch mehr um den Begriff als um die praktischen Vorschriften und eher auf Makro- als auf Mikroebene. Daher ist Forsthoffs Begriff von „Teilhaberecht als Beiordnung des Freiheitsrechts“ kein Konzept, das ganz selbstkonsistent, logisch selbstharmonisch, konnotativ klar und epitaxial definitiv ist (Luo Ying 2014).

3. Teilhaberecht als Derivat des Gleichheitsrechts

Unabhängig davon, ob Forsthoff das Teilhaberecht als Ersatz oder als Beiordnung zum Freiheitsrecht betrachtete, hatte seine Analyse subjektiv aus der Perspektive der Verwaltungsrechtswissenschaft und objektiv aus dem Blickwinkel der Verwaltungskunde darin eingeschnitten und dieser Einschnitt ging nicht aus der Perspektive der Menschenrechte oder der Verfassung. Forsthoffs Forschung zum Teilhaberecht dreht sich vor allem um das Konzept der „Daseinsvorsorge“, das nur ein wichtiger Bestandteil der Theorie der Dienstverwaltung ist. Im Gegensatz dazu basiert die Mainstream-Theorie der Teilhaberechte im heutigen Deutschland auf dem Grundgesetz der Bundesrepublik Deutschland und betont, dass das Teilhaberecht ein abgeleitetes Recht vom Gleichheitsrecht ist. Hier bedeutet das Teilhaberecht, dass diejenigen, die keinen Zugang haben, verlangen könnten, was auf der Grundlage des Rechts auf Gleichheit geteilt werden sollte, wenn der Staat einige Dienstleistungen für einige Menschen erbracht hat und die Verteilung jedoch ungerecht ist. Daher werden die Teilhaberechte auch als „abgeleitetes Recht zu Anspruch auf Leistungserbringung“ bezeichnet. D.h. das Teilhaberecht ist ein „Anspruch auf Leistungserbringung“, das sich als Derivat aus der Kombination der im Grundgesetz der Bundesrepublik Deutschland festgelegten Grundsätze des Sozialstaates und des Gleichheitsrechts ergibt. Diese Grundsätze des Sozialstaates betonen die soziale Verantwortung, die vom

Staat getragen und erfüllt werden sollte, das bedeutet, dass das Teilhaberecht einen bestimmten Raum hat. In der Zwischenzeit ist das Grundgesetz in Bezug auf die Frage der Grundrechte jedoch vorsichtig, sodass der Raum für das Bestehen der Teilhaberechte begrenzt ist. Basierend auf der Kombination der Grundsätze des Sozialstaates und des Gleichheitsrechts entsteht das Teilhaberecht als Derivat des Gleichheitsrechts, das sowohl im akademischen Kreis als auch bei den Praktikern breite Akzeptanz findet. Hier setzt das Teilhaberecht voraus, dass eine Dienstleistung objektiv existiert und ihre Grenze ist daher schon klar definiert. Darüber hinaus hat der Bundesgerichtshof Bedingungen und Umfang des Teilhaberechts festgelegt, demnach es nicht ausreichende Bedingung für Anspruch auf Teilhaberecht derjenigen ist, die diese Leistung nicht erhalten haben, wenn der Staat nur für einige aber nicht für andere Personen Dienstleistungen erbracht hat. Das Teilhaberecht derjenigen, die die Leistung nicht erhalten haben, kann nur dann abgeleitet werden, wenn das Versäumnis des Staates, Dienstleistungen für solche andere Personen zu erbringen, willkürlich ist oder gegen das spezifische diskriminierende Verbot gemäß der Verfassung verstößt (Zhao Hong 2010).

(IV) Grundlage der Legitimität der Teilhaberechte

Das traditionelle Sachenrechtssystem basiert auf Privateigentum und strebt den exklusiven Besitz der Dinge an. Das Privateigentum oder der exklusive Besitz von Dingen bildet einen wirksamen Anreizmechanismus, der die Kreativität der Menschen freisetzt und die effiziente Nutzung von Dingen fördert. Als eines der Ziele der Gesetzgebung zu Sachenrechten wurde das „Beste aus den Dingen machen“ jedoch bis heute nicht realisiert, während der offene Zugang und die Teilhabewirtschaft (Sharing Economy) im Gegenteil die Art und Weise verändert, wie Menschen Dinge nutzen, und sie dazu veranlasst, darüber nachzudenken, wie sie Dinge besser nutzen können. Im traditionellen Sachenrechtssystem wurde die Teilhabe aufgrund der „exklusiven“ Struktur von Sachenrechten und des Grundsatzes „ein Recht für ein Objekt“ nicht ausreichend berücksichtigt. Bei einer sorgfältigen Überprüfung der Geschichte und

des aktuellen Status der Sachenrechtsgesetze können wir jedoch deutlich erkennen, dass die Idee der Teilhabe schon lange in die Art und Weise eingedrungen ist, wie man Dinge verwendet und bereits zu einem grundlegenden und routinemäßigen Nutzungsmuster geworden ist (Schlüssel-Labor der Big-Data-Strategie 2018, S. 223).

Mit der kontinuierlichen Entwicklung der Gesellschaft sehen wir zwei Veränderungen in Bezug auf die Produktionsmittel: Einige Produktionsmittel sind immer reichlicher vorhanden, während andere knapper geworden sind. Für die spärlichen Produktionsmittel ist die Teilhabe sehr notwendig, da sie die Nutzungseffizienz solcher Produktionsmittel erhöhen kann, dadurch mehr Menschen Vorteile von den wenigen Produktionsmitteln ziehen können, wobei der wachsende Appetit der Menschen auf das, was knapp ist, zugleich eingedämmt wird. Für die reichlich vorhandenen Produktionsmittel sinken die Kosten kontinuierlich und werden sich schließlich null nähern, was die Exklusivität sinnlos macht und deren Teilhabe ist unvermeidlich geworden. Obwohl Daten eine Art knappe Produktionsmittel sind, können sie aber durch Teilhabe reichlich vorhanden werden und unendliche Vorteile generieren, ohne ihr Inhalt beschädigt zu werden. Die Kosten für Replikation und Teilhabe sind äußerst gering und können fast ignoriert werden (Schlüssel-Labor der Big-Data-Strategie 2018, S. 223). Für Daten ist daher das zentrale Anliegen die effiziente Nutzung, während die Teilhabe der wichtigste Ansatz ist.

Die technologische Entwicklung hat zugleich das ursprüngliche Bild verändert, in dem Maschinenbau und Chemie die zentrale Rolle spielen, wobei sie das derzeitige Gleichgewicht bei der Zinsverteilung brechen und das bestehende Rechtssystem schwer treffen. Einerseits ist das bestehende Rechtssystem nicht in der Lage, die bestehenden Probleme der Datensicherheit wirksam zu bewältigen, wobei die Menschen seit Langem von Gefahren der Datenverletzung usw. verworren werden. Andererseits beschränkt das bestehende Rechtssystem die regelmäßige Datenübertragung, was die Datenerfassung und die freie Meinungsäußerung etc. einschränkt und die Effizienz der Datennutzung verringert, sodass der Wert der Daten nicht effizient freigesetzt werden kann. Man hat Zweifel an der Anwendbarkeit und Rechtfertigung des bestehenden Rechtssystems geäußert und einige Probleme mit technologischen Mitteln gelöst. Bei Problemen mit

Datenrechten und -interessen ist die Technologie jedoch nur die äußere Ursache, während die interne Ursache in Widersprüchen zwischen verschiedenen Arten von Rechten an sich liegt. Das traditionelle Rechtssystem mit dem Besitz als sein Kern kann die Bedürfnisse im Verlauf der digitalen Zivilisation nicht mehr erfüllen. Es ist dringend erforderlich, ein neues Rechtssystem einzurichten, das sich auf die Teilhabe konzentriert, um eine Datenverbreitung mit Freiheit, Sicherheit und Gleichheit zu erzielen. Der Schlüssel dazu heißt das „Teilhaberecht“.

Mit Blick auf Wert haben Daten den Teilhabewert und darin liegt tatsächlich der größte Wert der Daten. Derzeit ist die Verteilung des Teilhabewerts jedoch unangemessen und auch nicht rational. Daten werden schwer ausgebeutet, was die Fortschritte der Liberalisierung und Gleichstellung der Daten erheblich einschränkt. Technologische Mittel haben nur begrenzte Auswirkungen auf die Verteilung des Teilhabewerts. Und eine grundlegende Lösung kann nur gefunden werden, wenn wir den Wert der Teilhabe als eine Art Recht definieren. Tatsächlich haben die Teilhaberechte bereits eine breite Akzeptanz als Grundrecht der Menschen im akademischen Kreis gefunden und werden schrittweise zu einem Konsens der gesamten Menschheit. Deshalb ist es für uns vernünftig und fundiert, das Konzept der „Teilhaberechte“ vorzuschlagen, um den Teilhabewert als Grundwert von Daten zu schützen und den Teilhabewert von Daten zu einem legitimen Recht zu machen.

Da Daten als Produktionsmittel die Umwandlung und Umstrukturierung der traditionellen Produktionsbeziehungen und sozialen Beziehungen vorantreiben, werden die Markttransaktionen für Verwirklichung der Arbeitsteilung und die Aufteilung knapper Ressourcen und Arbeitsleistungen nicht mehr benötigt. Bis dahin wird das Recht, Daten zu besitzen, an Wert verlieren und die menschliche Gesellschaft würde in eine neue Gesellschaftsordnung eintreten, die auf den Rechten der Teilhabe beruht. Die Teilhaberechte ermöglichen die Trennung von Eigentumsrecht und Nutzungsrecht und bilden ein auf der Teilhabe basierendes Entwicklungsmuster, in dem man „Daten nicht besitzen, sondern nutzen will“. Gleichzeitig ist die Teilhabe an Daten Voraussetzung für eine effektive Datennutzung, da ein „Datenelement mehrere Rechte haben“ kann und weil Daten von Natur aus immaterielle Objektivität und pluralistische

Subjektivität haben. Das Teilhaberecht ist daher eine notwendige Voraussetzung für die digitale Zivilisation.

Abschnitt II Ansprüche auf das Teilhaberecht

Datenrechte sind im Wesentlichen die Teilhaberechte. Auf der Grundlage der Teilhaberechte entsteht ein vollständiges und unabhängiges Datenrecht für die gleichen Daten, sodass Daten gleichzeitig von mehreren Subjekten kontrolliert und verwendet werden können und so kann der Wert der Daten erhöht werden. Traditionell werden Rechte auf der Grundlage des Egoismus festgelegt und dienen dem Schutz der eigenen Rechte. Im Gegensatz beruht das Teilhaberecht auf Altruismus und zielt darauf ab, den Teilhabewert der Daten zu schützen. Dank der extrem niedrigen Kosten für die Reproduktion schafft der Teilhabewert der Daten einen unendlichen Wert, der weit über dem primären Wert der Daten ist. Daher ist es viel wichtiger, den durch Teilhabe von Daten geschaffenen Wert zu schützen als den primären Wert von Daten zu schützen. Da es jedoch intensive Widersprüche und Konflikte zwischen den Teilhaberechten und dem Recht auf Privatsphäre bestehen, muss ein Gleichgewicht zwischen beiden hergestellt werden, um den Wert der Datenressourcen voll auszuschöpfen.

(I) Teilhaberecht: Essenz der Datenrechte

Das Gesetz schützt das Recht, während das Recht den Wert schützt. Der Zweck der Einrichtung von Datenrechten besteht darin, den Wert von Daten zu schützen. Daten haben ihren ursprünglichen Wert und Teilhabewert, der Letztere ist jedoch unbegrenzt und viel höher als der Erstere. Daher werden Datenrechte hauptsächlich zum Schutz des Letzteren verwendet. Neben dem Schutz soll das Datenrecht auch die kontinuierliche und gesunde Entwicklung der Datenindustrie fördern, so muss der Datenwert erhöht werden. Die Steigerung des primären Datenwerts

liegt aber in der Ausweitung der Produktion, während die Steigerung des Teilhabewerts der Daten von der stetigen Nutzung der Daten abhängt. Unter anderem sind die Kosten der Teilhabe weitaus niedriger als die für Erweiterung der Produktion. Deshalb liegt der Schlüssel zur Steigerung des Gesamtwerts von Daten in der Vermehrung des Teilhabewerts. Die Teilhaberechte sind somit zur Kern-Engine der Steigerung des Teilhabewerts von Daten und zur Essenz der Datenrechte geworden.

1. Teilhaberecht und Besitzrecht

Teilhabe und Besitz stellen den wesentlichen Unterschied zwischen Datenrechten und Sachenrechten dar. Zu den Rechten der Dinge gehören das Eigentumsrecht, das Nutzungsrecht, das Verdienstrecht und das Verfügungsrecht. Das Besitzrecht ist das Kontrollrecht auf Gegenstand und Kontrolle (Besitzrecht) ist die Grundlage des Eigentumsrechts. Ohne Besitzrecht würde Ausübung aller anderen drei Rechte beeinträchtigt. Nur wenn man wirklich das Besitzrecht hat, kann er das Nutzungsrecht, das Einkommensrecht und das Verfügungsrecht besser ausüben. Das in der menschlichen Gesellschaft entstandene Privateigentum und Einzelbesitz haben beide Besitz als Endziel. Mit dem Aufstieg der Sharing-Wirtschaft erkennt man jedoch, dass es nicht auf das Besitzrecht ankommt, sondern darauf, ob die Dinge wirklich von anderen genutzt werden können. Das Wesentliche der Teilhabe besteht darin, die Teilhabe an Nutzungsrecht und Einkommensrecht zu ermöglichen, um entsprechende Vorteile zu erzielen (He Zhe 2017). Die Übertragung des Nutzungsrechts hilft, das Beste aus ungenutzten Ressourcen herauszuholen. Die Prämisse dafür ist jedoch, dass das Subjekt des Eigentumsrechts, das das Besitzrecht hat, bereit ist, das Nutzungsrecht zu übertragen. Das Wesen bleibt immer noch im Besitz des „Besitzrechts“. Da das Wesen des Rechts der Dinge im Besitz liegt und die Wurzel in der Exklusivität der Dinge liegt, wird festgestellt, dass ein Objekt nicht mehrere Rechtssubjekte gleichzeitig haben kann. Der Besitz ist somit der einzige Weg, um das Recht der Dinge zu beherrschen.

Während der Übertragung vom Recht der Dinge könnten die Interessen des Rechtssubjekts wegen des Bestehens des Besitzrechts nicht

beeinträchtigt werden, da das Rechtssubjekt weiterhin über das Kontrollrecht auf dieses Ding verfügt. Im Gegensatz dazu können Daten mehrere Rechtssubjekte gleichzeitig haben, da sie mit extrem geringen Kosten und ohne Verlust unendlich reproduziert werden können. Unter solchen Umständen kann man Daten kontrollieren und verwenden, unabhängig davon, ob er das Recht hat, sie zu besitzen. Ohne das Besitzrecht kann man das Nutzungsrecht, das Einkommensrecht und das Verfügungsrecht auf Daten ebenso ausüben. Sobald das Nutzungsrecht auf Daten übertragen worden ist, nimmt die Partei, die sie erhält, die betreffenden Daten vollständig in Besitz. Diese Daten befinden sich jetzt außerhalb der Kontrolle ihres ursprünglichen Eigentümers. Nun ist das Besitzrecht auf Daten bedeutungslos. Es ist notwendig, Daten mit anderen zu teilen, wenn man möchte, Wert aus Daten zu schöpfen und ihn zu maximieren. Das würde unvermeidlich zu Konflikten mit dem Besitzrecht kommen. Daher sind das Teilhaberecht auf Daten und das Besitzrecht auf Dinge gleichermaßen wichtig. Dies ist das unvermeidliche Ergebnis der bestmöglichen Nutzung von Daten. Darüber hinaus liegt der wahre Wert von Daten in der unbegrenzten Reproduktion zu geringen Kosten, die die Grundlage der Entwicklung der digitalen Zivilisation bildet und bestimmt, dass die Teilhabe im Zeitalter von Big Data zu einer grundlegenden und zentralen Anforderung und das Teilhaberecht zum wesentlichen Recht von Daten wird. Sobald man von dieser Grundlage abweicht und das Recht der Dinge mechanisch für Datenrecht verallgemeinert, würde die Anwendung und Entwicklung von Daten erheblich behindert, was die ursprüngliche Absicht, Datenrecht für Datenschutz und -entwicklung zu etablieren, widersprechen und verletzen könnte (Schlüssel-Labor der Big-Data-Strategie 2018, S. 159).

2. Ein Recht für ein Ding im Vergleich zu mehreren Rechten auf einzelnen Daten

„Ein Recht für ein Ding“ ist das wesentliche Kennzeichen der Dominanz von Sachenrechten. Mit dem Fortschritt der Technologie hat das Ding mehrere Formen und dann entstanden nach und nach mehrere Arten von Sachenrechten, wobei die Unterscheidung zwischen Macht und Funktion des Eigentumsrechts immer komplizierter wird. Die Menschheit

verändert auch die Art und Weise, wie sie Dinge benutzt. In der Rechtspraxis kollidiert „ein Recht für ein Ding“ immer mehr mit „Mehrfache Rechte für ein Ding“ und „Ein Recht für mehrere Dinge“. Sie alle haben bis zu einem gewissen Grad eine indirekte Anerkennung oder eine vage gesetzliche Zustimmung erhalten, die von der ursprünglichen Bedeutung von „ein Recht für ein Ding“ abweichen. Im Gegensatz dazu können Daten wegen ihrer Immaterialität und Replizierbarkeit Interessen in mehreren Formen enthalten. Die Einrichtung des Teilhaberechts ermöglicht Daten, mehrere Rechtssubjekte zu haben, die nicht alle an dasselbe Datenrecht teilhaben, sondern sie haben jeweils separate und vollständige Datenrechte. Dies bildet das Muster der Teilhabe: „Man will es nicht besitzen, sondern nur nutzen“.

Da Daten Merkmale wie Replizierbarkeit, Nichtverbrauchbarkeit und besondere Gemeinsamkeit usw. aufweisen, können „mehrere Rechte auf einzige Daten“ existieren. Das bestimmt, dass man sich von der Idee der Entwicklung der Teilhabe abwenden würde, wenn irgendein Subjekt das absolute Verfügungsrecht auf Daten besitzen dürfte. Mit der Entwicklung der Zeit und den Fortschritten der Technologie wird der Besitz von Dingen nicht länger nötig, wenn die Kosten eines Objekts sinken und sich Null nähern. Dies gilt insbesondere für Datenressourcen, da diese reichlich vorhanden sind und keine Grenzkosten verursachen. Daher wird die Teilhabe an „Mehrfachrecht auf einzige Daten“ unweigerlich zu einem allgemeinen Trend. Langfristig werden viele knappe Ressourcen reichlich vorhanden sein, da die Teilhabe die Ressourcenknappheit weitgehend verändern wird. „Wenn wir aus technologischer Sicht diese Frage betrachten, sind nur wenige Ressourcen wirklich knapp. Die richtige Frage liegt vor allem darin, wie diese Ressourcen benutzt werden“ (Peter H. Diamandis & Steven Kotler 2014, S. 8).

3. Konnotation des Teilhaberechts

Das Teilhaberecht bietet einen Ansatz für Datenrecht, der ein Gleichgewicht zwischen öffentlichem und privatem Interesse herstellt und dazu beiträgt, die Kreativität der Bevölkerung anzuregen, sich für Entwicklung der digitalen Zivilisation einzusetzen. Der Kern des Teilhaberechts ist ein

ausgewogenes Verhältnis der Dateninteressen. Ob das öffentliche Interesse an Daten das private Interesse überwiegt oder umgekehrt, wird es gegen den Grundgeist von Freiheit und Gleichheit verstoßen. Jede unausgewogene Verteilung der Dateninteressen würde die Begeisterung und Initiative der Menschen vom Grund auf dämpfen, mit Daten Wohlstand zu schaffen. Die Bedeutung der Errichtung des Teilhaberechts besteht darin, den traditionellen Ansatz für Recht und Daten wie „Achtung auf private Interessen und Missachtung der Gemeinnützlichkei“ zu revidieren, und einen Ansatz für Datenrecht zu befürworten, der ein Gleichgewicht zwischen öffentlichem und privatem Interesse herstellt. Das Teilhaberecht ist Voraussetzung für die Datennutzung. Das ist sowohl die Grundanforderung an Aufbau der digitalen Zivilisation als auch der Hauptinhalt des Aufbaus einer neuen Gesellschaftsordnung (Long Rongyan & Yang Guanhua 2018).

Das Teilhaberecht ist ein wichtiger Bestandteil des Grundsystems der digitalen Zivilisation, wobei der Altruismus als grundlegende Basis dient. Aus Sicht der Gerechtigkeit ist die Verteilung zwischen öffentlichen und privaten Dateninteressen ein zentrales Thema in der digitalen Zivilisation. Erstens muss das Teilhaberecht dazu dienen, Gleichgewicht der Verteilung zwischen dem öffentlichen und privaten Bereich in Bezug auf Dateninteressen zu gewährleisten und dabei die Fairness aufzuweisen. Nur so können die Beziehungen zwischen den öffentlichen und privaten Dateninteressen der Datensubjekte gut ausgerichtet werden. Zweitens ist die Verteilung der öffentlichen und privaten Interessen von Daten absolut, objektiv und universell. Niemand darf beliebig nach seinen subjektiven Willen Vereinbarungen aufzwingen. Jede subjektive, relative oder übermäßige Interpretation zur Verteilung der öffentlichen und privaten Dateninteressen beeinträchtigt die Gerechtigkeit. Daher hat das Teilhaberecht eine äußerst wichtige realistische Bedeutung für den Aufbau einer neuen Ordnung der digitalen Zivilisation (Schlüssellabor der Big-Data-Strategie 2018, S. 225).

Das Teilhaberecht hilft bei der Schlichtung von Konflikten zwischen verschiedenen Datenrechtsinhabern und bietet eine Wertbasis für Beilegung von Streitigkeiten in Bezug auf Dateninteressen. Das Teilhaberecht soll das Gleichgewicht zwischen öffentlichen und privaten Dateninteressen wahren und die grundlegende Wertorientierung für Entwicklung

des Systems der digitalen Zivilisation bieten, damit der Gerechtigkeit hoher Prioritätswert im grundlegenden System der digitalen Zivilisation eingeräumt wird. Gemäß dem Grundsatz des Gleichgewichts zwischen öffentlichen und privaten Dateninteressen können Rechtsvorschriften zur Lösung von Konflikten zwischen Datenrechtsinhabern erlassen und Koordinierungsmechanismen für Interessenausgleich zwischen diesen Rechtssubjekten verbessert werden, um Kanäle ungehindert zu öffnen, durch die die Datenrechtssubjekte ihre Ansprüche auf Dateninteressen erheben und verschiedene soziale Krisen zu entschärfen, die durch Konflikte zwischen Dateninteressen verursacht werden. Auf diese Weise können Datenrechtssubjekte „alles tun, was sie können, und das bekommen, was sie bekommen sollen“. Gleichzeitig kann das Teilhaberecht auch dazu beitragen, Probleme wie unfaire Zuweisung von Ressourcen, Ungleichheit der Chancen und soziale Ungerechtigkeit etc., die durch das Datenmonopol verursacht werden, zu lösen, soziale Fairness und Gerechtigkeit zu gewährleisten, eine optimale Zuweisung von Datenressourcen und null Grenzkosten zu erreichen, Wohlstand von Daten zu vermehren und harmonische Entwicklung der Wirtschaft und Gesellschaft im Zeitalter der digitalen Zivilisation zu fördern.

(II) Logischer Ausgangspunkt der Teilhaberechte

Das Teilhaberecht ist eine Art von Rechten, die dem Besitzrecht entgegengesetzt sind. Was das Besitzrecht schützt, sind Interessen der Dateninhaber und Interessen, die basiert auf Egoismus entstehen. Bis zu einem gewissen Grad dient das Besitzrecht als grundlegende Triebkraft für den Ausbau der Datenproduktion. Die Menschheit kann jedoch Datenressourcen ohne Einschränkung produzieren, und der Besitz von Daten führt zwangsläufig zu einer enormen Verschwendung von Ressourcen. Das determiniert, dass das Datenbesitzrecht die Anforderungen der Datenentwicklung nicht erfüllen kann. Die objektive Tatsache der Knappheit unterstreicht noch mehr den Altruismus der Entwicklung. Aufgrund der extrem niedrigen Kosten für Datenreproduktion besteht eine natürliche Verbindung zwischen Daten und Teilhabe. Das Teilhaberecht wird

schließlich das Besitzrecht ersetzen und zur zentralen Triebkraft für die Entwicklung der digitalen Zivilisation werden. Als ein Recht entsteht das Teilhaberecht auf der Basis des Altruismus, nimmt den Altruismus als seine konzeptionelle Grundlage und prägt die Denkweise der Menschen für Datenteilhabe, lassen andere Menschen zur Anwendung an Daten teilhaben und gräbt den Teilhabewert von Daten aus. In diesem Sinne kann man sagen, dass der Altruismus der logische Ausgangspunkt des Teilhaberechts ist.

Altruismus der Datenrechte. Der Altruismus wird traditionell als typisches Merkmal moralischen Verhaltens angesehen. Auf dem Gebiet des Gesetzes manifestiert es sich jedoch lediglich in einer kleinen Anzahl von Handlungen, die darauf abzielen, „Guter Samariter aus Gerechtigkeitssinn“ und „den Bedürftigen helfen“ usw. Im Allgemeinen ist der Altruismus eher ein moralisches Streben, während der Egoismus im Gesetz vorherrscht. Angesichts des grundlegenden Attributs eines Datenmenschen kann die egoistische Eigenschaft eines Datenmenschen jedoch keine ausreichende Unterstützung erhalten. Der Grund dafür liegt darin, dass Datenmenschen der Menschlichkeit dabei helfen können, besser zu arbeiten und zu leben, ihr instrumenteller Wert bestimmt, dass sie von der Natur altruistisch sind. Der Altruismus eines Datenmenschen hat der Menschheit enorme Vorteile gebracht. Bei der Verfolgung von Interessen entscheidet man sich für Interaktion mit Datenmenschen, damit es zu mehreren altruistischen Verhaltensweisen kommen kann. Wenn Datenmenschen die notwendige Rechtsgrundlage auf dem gesetzlichen Gebiet erhalten, werden altruistische Verhaltensweisen einen tief greifenden Einfluss auf die Art der Datenrechte üben. Einige Wissenschaftler glauben, dass sich die Arten mit altruistischer Tendenz im Wettbewerb im Ökosystem in einer nachteiligen Stellung befinden und ihre soziale Anpassungsfähigkeiten auch dadurch verringert werden könnten (Li Jianhui & Gong Xiaole 2009). Die Interdisziplinäre Studien zur Spieltheorie und zum biologischen Evolutionismus zeigen jedoch, dass die Artengruppe mit altruistischem Geist im Vergleich zu selbstsüchtiger Artengruppe mehr evolutionäre Vorteile im Wettbewerb im Ökosystem haben (Liu Heling 2005). Aus diesem Grund bildet der altruistische Charakter von Datenrechten nicht unbedingt einen Nachteil im Wettbewerb um Rechte. Im Gegensatz fördert er vielmehr die

menschliche Entwicklung. Außerdem ist der Altruismus der Datenrechte auch hilfreich für die Förderung der Interaktion zwischen Menschen und Datenmenschen. Indem ein Datenmensch etwas Altruistisches tut, sendet er ein Signal zur Interaktion aus, um mehr Handlungsspielraum und mehr Möglichkeiten zur Zusammenarbeit zu schaffen. Davon profitieren zunächst nur wenige Menschen, die damit Geld verdienen können. Wenn mehr Menschen daran teilnehmen, können die altruistischen Handlungen von den zufälligen Interaktionsbeziehungen auf bestimmten gesetzlichen Beziehungen steigen und somit sichergestellt werden, dass die Menschheit aus altruistischen Handlungen langfristig stetige Erfolge erzielen kann. Um das Wohlergehen der Daten in der Gesellschaft zu verbessern und den menschlichen Fortschritt zu fördern, muss der Staat Mechanismen zum Schutz „altruistischer Verhaltensweisen“ einrichten, d.h. das Recht auf Altruismus festlegen. Das ist eine Art Recht, dessen Eigenschaft sowohl die des empfohlenen Rechts der Datenmenschen ist, das aufgrund der Entwicklungsbedürfnisse der Menschheit anerkannt wird, als auch das gesetzliche Signierung der altruistischen Funktionen der Datenmenschen darstellt (Zhang Yujie 2017).

Altruismus und Teilhabe an Datenrechten. Im Zeitalter von Big Data fördert die Datenteilhabe als typisches Verhalten außerhalb der Rolle die Entwicklung von Teams und Organisationen erheblich. Wenn aber Wettbewerbsbeziehungen zwischen Einzelpersonen innerhalb einer Organisation bestehen, könnte die Datenteilhabe das Recht und Interesse der Einzelpersonen schädigen. Aus Berücksichtigung der Eigeninteressen neigen Menschen daher dazu, keine Initiative zu ergreifen, um Daten gemeinsam zu nutzen. Unter solchen Umständen wird die Teilhabe an Daten durch Einzelpersonen hauptsächlich vom Altruismus angetrieben, die sich in den folgenden vier Aspekten manifestiert: Erstens ist das Wesen von Einzelpersonen, anderen zu helfen, oder insbesondere die Bereitschaft von Einzelpersonen, Daten ohne Vergütung mit anderen zu teilen. Zweitens ist der gegenseitige Altruismus, ein typisches Beispiel dafür ist die prosoziale Zusammenarbeit und gegenseitige Hilfe, die die Einzelperson in der Gesellschaft menschlicher Beziehungen zeigt. Drittens ist der reputationsorientierte Altruismus, der durch Neigung zum „guten Menschen“ in der Struktur der menschlichen Wertanschauung dargestellt wird, die die

Menschen zu altruistischen Verhaltensweisen führt, um ihren Ruf oder ihre eigentlich gebührende Werterwartung aufrechtzuerhalten. Viertens ist die gezwungene Datenteilhabe, die zum Beispiel gemäß den Anweisungen der Vorgesetzten geschehen kann. Daraus ist ersichtlich, dass der Altruismus das individuelle prosoziale Verhalten (z. B. Zusammenarbeit, Maßnahmen zum gegenseitigen Nutzen, Hilfe für andere usw.) erheblich fördert (Zheng Jianjun & Fu Xiaojie 2019). In Bezug auf das Wesen ist das Teilhaberecht naturgemäß eindeutig prosozial und stellt Verhaltensweisen außerhalb der Rolle dar, die für die Entwicklung einer Organisation hilfreich sind. Das Teilhaberecht ist also eine wichtige Dimension des Verhaltens eines Unternehmensbürgers. D.h. insgesamt hat das Teilhaberecht die übereinstimmenden Merkmale mit den Verhaltensweisen wie prosoziales, hilfsbereites, kooperatives und selbstloses Verhalten usw. Der Altruismus hat daher einen erheblichen positiven Einfluss auf die Bereitschaft und das Handeln der Menschen für Datenteilhabe. Das Wesen der Teilhabe ist Altruismus, der eine unentbehrliche Bedingung und Grundlage für Verwirklichung der Teilhaberechte bietet. Der Altruismus als verinnerlichtes spirituelles Bedürfnis und als veräußerlichtes bewusstes Handeln bringt anderen tendenziell Vorteile. Im Zeitalter von Big Data liegt die ultimative Bedeutung des Altruismus in der Förderung der Integration zwischen Datenrechten und der Nutzung, dem Schutz und dem Wert von Daten. Die Wertansicht des Altruismus verbessert die subjektive Bereitschaft der Menschen, Datenrechte zu übertragen und gemeinsam zu nutzen, erleichtert die Einrichtung von Teilhaberechten und trägt dazu bei, die Übertragung und Teilhabe von Daten zu einer Aktion von äußerst positiver Bedeutung zu machen.

Das Teilhaberecht des Datenmenschen. Die Grundrechte werden traditionell als grundlegendste und Kernbestandteil der Bürgerrechte betrachtet, und die Grundlage für ihre Existenz sind die Grundwerte und Universalität der Rechte. In diesem Sinne bietet das Teilhaberecht als Grundrecht eines Datenmenschen die notwendige Garantie für die Datenmensch-Hypothese. Die Teilhaberechte sind das primäre Grundrecht eines Datenmenschen. Im Moment gibt es aber einige eindeutige Konflikte zwischen dem Schutz der Teilhaberechte und dem Schutz anderer Rechte. Einerseits neigen die allgemeine Öffentlichkeit und Unternehmensorganisationen dazu, ihre Datenrechte geltend zu machen und Schutz für sie aktiv

zu suchen (z. B. das Recht auf Vergessen und Rechte an Dateneigentum etc.), da Datenressourcen einen kommerziellen Wert und möglicherweise auch Informationen der persönlichen Geheimnisse und sogar Informationen der staatlichen Sicherheit enthalten. Dies wird den Umfang der Datenteilhabe verringern und so die Verwirklichung der Funktionen der Teilhaberechte benachteiligen. Andererseits ist ein Datenmensch stark auf Datenanalyse angewiesen. Ohne das Teilhaberecht könnten Datenmenschen mehrere Verletzungsrisiken passieren. Sollte das Gesetz daher die Bürgerrechte schützen oder die Aufforderungen der Datenmenschen auf Teilhabe an Datenrechte unterstützen? Was auch immer die Wahl wäre, würde sich die andere Seite, die ungeschützt bleibt, wahrscheinlich hart wehren. Obwohl die Privatsphäre jetzt bis zu einem gewissen Grad geschützt werden kann, gehen die sozialen Veränderungen, die durch das Teilhaberecht entstehen, weit über das hinaus, was am Wert des Datenschutzes gemessen werden kann. In der Zwischenzeit hat der Datenrechtsschutz, der im Bereich der privaten Rechte floriert, im Bereich der öffentlichen Rechte nur minimale Erfolge erzielt. Nichts anderes als die Ausübung des Teilhaberechts repräsentiert den allgemeinen Entwicklungstrend in der zukünftigen digitalen Zivilisation. In diesem Sinne sollen aus gesetzlicher Sicht daher Anstrengungen in den folgenden zwei Aspekten unternommen werden: Erstens sollen Daten sowohl zum Geheimnisschutz als auch zur Offenlegung klar klassifiziert werden, um die Datenschutzrechte der Privatsphäre von Bürgern und Geschäftsgeheimnisse von Unternehmensverbänden zu schützen. Zweitens sollen Anstrengungen unternommen werden, um die gemeinsame Nutzung von Datenressourcen in allen Formen zu fördern, das Teilhaberecht von Datenmenschen zu bekräftigen und Rechtskonflikte zu vermindern.

(III) Balance zwischen dem Teilhaberecht und dem Recht auf Privatsphäre

Verwirklichung der Datenzirkulation und Datenteilhabe ist die unvermeidliche Wahl für die Modernisierung der Industrie, wissenschaftliche und technologische Innovationen und Erhöhung der

Verwaltungsfähigkeit der Regierung im Zeitalter der digitalen Zivilisation. Es gibt jedoch natürliche Interessenkonflikte zwischen Datenteilhabe und Datenschutz der Privatsphäre, während die Spannung der Beziehung zwischen beiden nach und nach zunimmt. Dies ergibt sich aus dem Spiel zwischen öffentlichen und persönlichen Dateninteressen und aus der Divergenz zwischen Eigentumsinteressen und Persönlichkeitsinteressen von Daten. Daher muss das Gleichgewicht zwischen den Teilhaberechten und dem Recht auf Privatsphäre hergestellt werden, um den Wert der Datenressourcen vollständig auszugraben.

Öffentliche Interessen gegen persönliche Interessen. Die Konflikte zwischen dem Teilhaberecht und dem Recht auf Privatsphäre sind zum Teil auf das Spiel zwischen öffentlichen Interessen und persönlichen Interessen von Daten zurückzuführen. Einerseits weisen die Teilhaberechte in Bezug sowohl auf ihre Zwecke und als auch auf ihre Funktionen eindeutig die öffentliche Eigenschaft auf. Der Zweck der Erstellung der Teilhaberechte besteht darin, die Teilhabe an Datenressourcen zu fördern, Datenressourcen besser zu aktivieren und den freien Verkehr und die gemeinsame Nutzung von Daten zwischen Regierungen, Unternehmen und der Öffentlichkeit zu realisieren. Aus funktionaler Sicht besitzen Daten einen enormen wirtschaftlichen und sozialen Wert. Der freie Verkehr und die Teilhabe von Daten tragen zur schnellen Umgestaltung der Regierungsfunktionen, zur Erhöhung der Verwaltungsfähigkeit der Regierung und zur Steigerung der Qualität der öffentlichen Dienstleistung bei. Zugleich bildet die Datenteilhabe eine solide Datenbasis für die industrielle Entwicklung, ermöglicht es Kunden, rechtzeitige und gezieltere Dienstleistung in Anspruch zu nehmen, spart Kosten der Zeit und Energie, fördert die optimierte Zuweisung sozialer Ressourcen und steigert die Effizienz der Nutzung von Datenressourcen. Andererseits bekräftigt das Recht auf Privatsphäre von Anfang an immer „ohne Einmischung von anderen“ und zielt auf den Schutz des Rechts der Einzelnen auf privaten Raum vor fremder Einmischung ab. Dies zeigt deutliche Merkmale der Autonomie des Privatrechts. Mit der sozialen Entwicklung und dem wissenschaftlichen und technologischen Fortschritt wird die Konnotation des Rechts auf Privatsphäre schrittweise auf Bereiche wie Privatsphäre der Selbstbestimmung, des privaten Raums und der Informationen etc.

ausgedehnt. „Jede Privatsphäre, die eine Person nicht offenlegen möchte, soll auf der Grundlage des Rechts auf Privatsphäre geschützt werden, ganz egal, ob die Offenlegung dieser privaten Daten positiv oder negativ auf den Rechteinhaber auswirkt, solange diese Daten nicht zum öffentlichen Bereich gehören und solange er persönlich nicht bereit ist, sie gemeinsam nutzen zu lassen“ (Zhang Xinbao 1998, S. 21). Das Recht auf Privatsphäre stellt immer den Schutz der persönlichen Würde und Autonomie in erster Linie, damit Einzelpersonen einige Informationen für sich behalten und aufbewahren können, die ihnen helfen können, dem Druck von außen zu widerstehen und ihre eigenen Interessen zu schützen. Wie Professor Wang Liming einmal sagte, ist das Recht auf Privatsphäre in gewissem Maße natürlich „antisozial“. Es trennt den Bereich der Privatsphäre vom Bereich der Öffentlichkeit, sodass der Einzelne sein Leben ohne Störung alleine ruhig genießen kann. In gewissem Maße widerspricht dies dem, was die Gesellschaft bevorzugt (Wang Liming 2005, S. 604). Konflikte zwischen dem Recht auf Teilhabe, das die schwere Verantwortung für industrielle und soziale Entwicklung schultert, und dem Recht auf Privatsphäre, das die gesetzlichen Rechte und Interessen des Einzelnen wahrt, ergeben sich daher im Wesentlichen aus dem Spiel zwischen den öffentlichen Interessen und persönlichen Interessen im Prozess dieser zirkulierenden Teilhabe wie „Datensammlung-Datennutzung-Datenumlauf“.

Unterschiede zwischen Eigentumsinteressen und Persönlichkeitsinteressen. Ein weiterer Grund für die Konflikte zwischen dem Teilhaberecht und dem Recht auf Privatsphäre liegt in der Diskrepanz zwischen Eigentumsinteressen von Daten und Persönlichkeitsinteressen von Daten. Einerseits ist es nicht realistisch, Daten so zu behandeln, dass sie nur einen Persönlichkeitswert haben, da die in Daten enthaltenen Eigentumsinteressen an Bedeutung gewinnen und die kommerziellen Datenaktivitäten stets zunehmen. Daten enthalten sowohl Eigentumsinteressen als auch Persönlichkeitsinteressen und sind bereits zu einer Art von rentablem immateriellem Vermögen geworden. Wir sollen uns voll und ganz bewusst sein, dass Daten als Eigentum betrachtet werden können und ihre Rolle als Motor für das Wirtschaftswachstum besser spielen können. Andererseits betont das traditionelle Recht auf Privatsphäre den Schutz von Daten auf der Grundlage des darin enthaltenen Persönlichkeitswertes. Der

Persönlichkeitswert von Daten ist ebenso wichtig wie ihr Eigentumswert. Daten werden Tag um Tag ständig generiert und durch Teilhabe gesammelt und bilden ein detailliertes Profil unseres „täglichen Lebens wie Kleiden, Essen, Wohnen und Verkehren und sogar unserer zukünftigen Aktivität“. Eine solche Beschreibung ist tendenziell genauer als die Beschreibung, die wir über unser eigenes Leben geben können. Die Datenteilhabe hilft uns daher, das Leben der Menschen und sogar ihren mentalen Zustand besser zu betrachten, sodass jeder jederzeit in einem Panoptikum, genannt als „Rundes Gefängnis“ überwacht wird. Die Freiheit der Menschen, ihren Lebensstil selbstständig zu wählen, der freie Wille für eigene alltägliche Angelegenheiten, Geheimnisse und Frieden in ihrem privaten Bereich und die Kontrolle über ihre eigenen Daten können durch Datenteilhabe verletzt werden. Man kann sich sogar unsicher fühlen, ob die Wahl von ihnen selbst oder von Daten getroffen wird. Daten bringen daher doppelte Interessen mit sich: Die Datenteilhabe konzentriert sich auf den Schutz der Eigentumsinteressen von Daten, während der Schutz der Privatsphäre den Persönlichkeitsinteressen von Daten mehr Aufmerksamkeit schenkt. Die Diskrepanz zwischen beiden hinsichtlich des Interessenschutzes führt zu Konflikten zwischen dem Teilhaberecht und dem Recht auf Privatsphäre (Wang Yan & Ye Ming 2019).

Weg zum Gleichgewicht zwischen dem Teilhaberecht und dem Recht auf Privatsphäre. Die Festlegung der Verteilung und Beilegung von Streitigkeiten ist eine der Grundfunktionen des Gesetzes. Um diese Funktion zu realisieren, muss das Gesetz ein Gleichgewicht zwischen mehreren Arten von Interessen anstreben. Genauer gesagt betont das Teilhaberecht den freien Verkehr und Teilhabe an Daten und vertreten öffentliche Interessen und Eigentumsinteressen. Im Gegenteil vertritt das Recht auf Privatsphäre private Interessen und Persönlichkeitsinteressen. Konflikte zwischen diesen beiden Seiten sind unvermeidlich. Trotzdem sind sie beiden nicht völlig gegensätzlich. Bis zu einem gewissen Grad sind die Ansprüche auf öffentlichen und die auf privaten Interessen übereinstimmend: Die öffentlichen Interessen sind Summe der universellen privaten Interessen. Zugleich schließt der Schutz der Eigentumsinteressen der Rechteinhaber den Schutz ihrer Persönlichkeitsinteressen nicht aus. Wenn wir uns also mit Konflikten zwischen dem Teilhaberecht und dem

Recht auf Privatsphäre befassen, reicht es nicht aus, einer Seite Vorrang einfach einzuräumen, sondern müssen wir ein Gleichgewicht zwischen öffentlichen und privaten Interessen sowie zwischen Eigentumsinteressen und Persönlichkeitsinteressen finden. Mit anderen Worten, das Datenschutzgesetz soll nicht nur die Persönlichkeit und Würde der Einzelnen schützen, sondern auch den wirksamen Betrieb des Teilhaberechts berücksichtigen, indem das Recht auf Privatsphäre einigermaßen eingeschränkt wird. Gleichzeitig sind das Teilhaberechtsrecht und das Recht auf Privatsphäre wie die beiden Seiten einer Münze. Um die öffentlichen Interessen zu wahren und die wirtschaftliche Entwicklung zu fördern, ist es notwendig, den freien Datenverkehr und Datenteilhabe zwischen Regierungen, Unternehmen und der Öffentlichkeit zu verwirklichen. Hier sollen einige Einschränkungen und Verringerungen hinsichtlich des Rechts auf Privatsphäre vorgenommen werden, um einige nicht zum Kern gehörende Interessen dem Teilhaberecht zu übertragen und die Grundbedingungen für Teilhaberechte zur Verwirklichung ihrer Kerninteressen zu gewährleisten. Gleichzeitig darf das Teilhaberecht auch nicht ungehindert wild wachsen. Es sollen auch gebührende Einschränkungen vom Recht auf Privatsphäre auferlegt werden, damit das Recht auf Privatsphäre angemessen gewährleistet werden kann. Wenn man jedoch die bestehenden Gesetze vieler Länder untersucht, kann man feststellen, dass die Gesetzgebung zu Daten weit hinter den realen Erfordernissen der Entwicklung der Datenindustrie zurückbleibt. Um den Anforderungen der Praxis und der theoretischen Entwicklung gerecht zu werden und Doppelgewinn-Ergebnisse für die Datennutzung und den Datenschutz zu erzielen, ist es daher notwendig, so bald wie möglich ein Datenschutzgesetz zu formulieren, um Konflikt zwischen dem Teilhaberecht und dem Recht auf Privatsphäre durch Gesetzgebung zu schlichten, sich mit grundlegenden Fragen in Bezug auf das Teilhaberecht und das Recht auf Privatsphäre zu befassen, den Umfang und die Grenze der Rechte klar zu definieren, strenge Regeln für die Verwirklichung des Teilhaberechts festzulegen, die Aufsicht über die Ausübung des Teilhaberechts zu verstärken und entsprechende Verantwortungs- und Rechtsbehelfsmechanismen für Haftung in Bezug auf Datenschutzverletzung der Privatsphäre durch das Teilhaberecht festzusetzen und zu vervollständigen.

Abschnitt III Inhalt der Teilhaberechte

Aufgrund seines Attributs können wir das Teilhaberecht in drei Arten einteilen: das Teilhaberecht an öffentlichen Daten, Teilhaberecht an Geschäftsdaten und Teilhaberecht an persönlichen Daten. Durch Spezifizierung der Teilhaberechte auf Grundlage dieser Klassifizierung werden wir die freie und ordnungsgemäße Entwicklung der Datenteilhabe realisieren und den Datenteilhabewert erhöhen. Gleichzeitig werden die Datenrechte auf Grundlage der Erweiterung der Funktionen der Rechte der Dinge in vier Teilfunktionen eingeteilt, nämlich: Zugriffsrecht auf Teilhabedaten, Nutzungsrecht auf Teilhabedaten, Ertragsrecht auf Teilhabedaten und Verfügungsrecht auf Teilhabedaten und so wird eine Grundlage für die Ausübung des Teilhaberechts geboten. Daten können jedoch auch in öffentliche und nicht öffentliche Daten unterteilt werden. Um diese beiden Datentypen optimal nutzen zu können, trennen wir die Funktionen der Teilhaberechte und errichten gemeinnützige Datenrechte und Nutznießdatenrechte, die die grundlegenden Methoden zur Verwirklichung der Teilhaberechte darstellen.

(I) Arten der Teilhaberechte

Die Einführung des Teilhaberechts an öffentlichen Daten bricht einerseits die „Dateninsel“ des öffentlichen Sektors durch Datenteilhabe und setzt andererseits Dividenden von öffentlichen Daten durch offenen Zugang zu Daten frei. Geschäftsdaten machen im Vergleich zu den beiden anderen Typen einen relativ geringen Anteil an der Gesamtdatenmenge aus, aber unter bestimmten Bedingungen können sowohl öffentliche Daten als auch personenbezogene Daten in Geschäftsdaten umgewandelt werden. Geschäftsdaten, die auf wirtschaftlichen Aktivitäten auf dem Markt basieren, haben daher das größte Entwicklungspotenzial. Die Einrichtung des Teilhaberechts auf Geschäftsdaten kann die Umwandlung in Geschäftsdaten fördern, den Umfang der Datentransaktion verbreitern und den Nutzungswert von Daten vermehren.

Personenbezogene Daten enthalten einen enormen Wert. Die Einrichtung des Teilhaberechts auf personenbezogenen Daten stellt die Vorteile, die Menschen durch Datenteilhabe erzielen können, sicher und motiviert die persönliche Tatkraft, mehr Daten zu produzieren und daran teilzuhaben.

1. Das Teilhaberecht an öffentlichen Daten

Das Teilhaberecht an öffentlichen Daten ist das Recht auf Teilhabe an öffentlichen Daten. Die sogenannten öffentlichen Daten im juristischen Sinne beziehen sich auf Datenressourcen, die in engem Zusammenhang mit öffentlichen Interessen stehen. Daten in Bezug auf Regierungsangelegenheiten sind der wichtigste und größte Teil der öffentlichen Daten, da die Regierung bei der Wahrnehmung öffentlicher Aufgaben massive Datenressourcen sammeln kann. Laut Statistik verfügt die Regierung über 80 Prozent aller Datenressourcen. Da die öffentlichen Daten jedoch vielmehr auf verschiedene Regierungsabteilungen verteilt sind, so ist eine große Anzahl von „Dateninseln“ gebildet worden. Darüber hinaus fehlt den Menschen manchmal die Motivation, ihre Daten zu teilen, da die Interessen der verschiedenen Abteilungen einbezogen werden. Infolgedessen entsteht schließlich ein Regierungsmonopol, das wegen schlechter Datenintegration ernsthafte Verschwendung verursacht. Gleichzeitig führt die Datenbewegung unter dem Einfluss des Matthew-Effekts tendenziell zu einer „Datenkluft“, und die Öffentlichkeit, die normalerweise am Rand gedrängt wird, kann die von Daten gebrachten Dividende möglicherweise nicht in vollem Umfang genießen. Dies könnte der Öffentlichkeit immer mehr das Gefühl geben, „ihre Datenrechte relativ ausgebeutet zu werden“. Im Wesentlichen sind öffentliche Daten jedoch öffentliches Eigentum, das der ganzen Bevölkerung gehört. Unter der Voraussetzung, Privatsphäre, Geschäftsgeheimnisse und staatliche Sicherheit zu gewährleisten, soll der Staat diese Daten an die ganzen Volksmassen zurückgeben. In diesem Sinne stellt die Einführung des Teilhaberechts an öffentlichen Daten eine Teilhabe-Bewegung dar, bei der die Volksmassen ihre Rechte an öffentlichen Daten von Regierungsbehörden beanspruchen. Gleichzeitig ist es angesichts des Erwachens des Bewusstseins der

Öffentlichkeit für ihre Datenrechte unerlässlich, das Teilhaberecht an öffentlichen Daten dringendst festzulegen.

Das Teilhaberecht auf öffentlichen Daten ist ein grundlegendes Bürgerrecht, das es der Gesellschaft ermöglicht, öffentliche Datenressourcen zu kontrollieren und zu nutzen. Dieses Recht ergibt sich einerseits aus der Verpflichtung der Menschen, die Datenerfassung zu akzeptieren und zu unterstützen, und andererseits aus der Tatsache, dass öffentliche Daten in der Natur dem gesamten Volk gehören. Unter normalen Umständen hat man das Recht, alle öffentlichen Daten mit Ausnahme sensibler Daten wie Privatsphäre, Geschäftsgeheimnisse und Informationen über Staatssicherheit zu wissen, zu verwenden und daran teilzuhaben. Daher kann das Teilhaberecht auf öffentlichen Daten in zwei Arten unterteilt werden. Eine ist das Recht auf Teilhabe an Daten im öffentlichen Sektor oder einfach als das „Teilhaberecht auf Abteilungsdaten“ genannt. Es fördert den freien Verkehr öffentlicher Daten im öffentlichen Sektor, trägt dazu bei, Hindernisse wie streifen- und stückförmige Verteilung zwischen höheren und niedrigeren Ebenen sowie zwischen verschiedenen Abteilungen des öffentlichen Sektors abzubauen, damit mehr Datenressourcen gemeinsam genutzt werden können. Die andere ist das Recht, Daten für die gesamte Gesellschaft offen zu machen, oder kurz genannt als Recht auf „offenen Zugang zu öffentlichen Daten“ anzubieten. Im Vergleich zu Teilhabedaten sind Daten für offenen Zugang relativ klein, da einige öffentliche Daten vertraulich behandelt werden müssen und für die Öffentlichkeit nicht zugänglich sind.

Das Teilhaberecht auf öffentlichen Daten betont die Verfolgung des Werts, den man über öffentliche Daten wissen will. Dabei handelt es sich jedoch nicht um eine Kopie oder aktualisierte Version des Wissensrechts der Bürger im Bereich der öffentlichen Daten. Das Recht der Bürger auf Wissen bedeutet, dass Bürger gesetzmäßig das Recht haben, die Offenlegung einiger Informationen durch staatliche Organe zu verlangen. Es konzentriert sich auf Erhalten von und Informiert-Werden über Regierungsinformationen und soll zum Aufbau einer offenen Regierung beitragen. Im Gegensatz dazu betont das Teilhaberecht auf öffentlichen Daten die Teilhabe an und Nutzung von öffentlichen Daten: Einerseits geht der Zweck der Nachfrage der Menschen nach öffentlichen Daten

seit Langem über eine bessere Transparenz der Regierungsoperationen hinaus. Es geht jetzt vielmehr um Schaffung von sozialem und wirtschaftlichem Wert durch Nutzung und Ausgrabung von öffentlichen Daten. Andererseits erfordert das Teilhaberecht auf öffentlichen Daten, dass der öffentliche Sektor die Initiative ergreift, um Daten unverzüglich weiterzugeben, und es stellt die Aktualisierung des Ansatzes des öffentlichen Dienstes von der passiven Offenlegung bei Informationsanspruch zur positiven Weitergabe ohne Aufforderung dar. Obwohl das Teilhaberecht auf öffentlichen Daten in der Rechtstheorie zwar nicht direkt oder ausdrücklich dargelegt wurde, verhindert dies jedoch nicht, dass das Teilhaberecht auf öffentlichen Daten zu einem grundlegenden Bürgerrecht wird. In Bezug auf die Abdeckung ist das Teilhaberecht auf öffentlichen Daten im Wesentlichen ein Rechtsbündel, die sich aus dem Mehrwert ergeben, der durch Teilhabe an öffentlichen Daten entsteht. Aus dieser Perspektive gilt das Teilhaberecht auf öffentlichen Daten als ein bürgerliches Recht, das darauf abzielt, an die Ergebnisse der Entwicklung öffentlicher Daten teilzuhaben, im Wesentlichen als eine Mischung aus Rechten. Dies kann sowohl das Entwicklungsrecht auf der Grundlage von Ertragsteilhabe oder das Aufsichtsrecht auf datengesteuerte Verwaltung oder das Recht auf Teilnahme zur Überbrückung der Informationsasymmetrie sein (Cheng Tongshun & Shi Meng 2018).

2. Das Teilhaberecht auf Geschäftsdaten

Während ihrer Produktions- und Betriebsprozesse sammeln Unternehmen große Mengen Geschäftsdaten, die in zwei Teile unterteilt werden können. Einer davon sind Geschäftsdaten in Bezug auf Identitätseigenschaften und Verhaltensmerkmale von Verbrauchern, die das Eigentum der betreffenden Personen sind und von den Unternehmen nicht verkauft oder übertragen werden dürfen. Der andere sind Verbrauchsdaten, die von Unternehmen erhalten wurden. Dieser Teil der Daten kann nach Zusammenfassung, Desensibilisierung und Entschlüsselung als Geschäftsdaten der betreffenden Unternehmen angesehen und von den Unternehmen als solche verfügt oder gehandelt werden. Diese Kategorisierung ermöglicht es Unternehmen, Geschäftsdaten kontinuierlich und

ordnungsgemäß zu handeln, während das Teilhaberecht auf Geschäftsdaten dazu beiträgt, den potenziellen Wert von Geschäftsdaten stets freizusetzen.

Der Wert von Daten liegt darin, ständig verwendet, analysiert und abgebaut zu werden. Die Nichtverbrauchbarkeit der Daten stellt sicher, dass je mehr Daten verwendet werden, desto mehr Interessen entstehen, während das Risiko eines Verlusts von Geschäftsgeheimnissen auch gleichzeitig steigen könnte. Je mehr potenzieller Wert aus Geschäftsdaten entdeckt wird, desto mehr Aufmerksamkeit gewinnen Daten als Ressource oder Vermögen. Viele Unternehmen kaufen Geschäftsdaten, um Gewinne daraus zu erzielen. Unternehmen mit Geschäftsdaten halten es jedoch für selbstverständlich, dass sie in ihrem Unterbewusstsein die von ihnen aggregierten Daten besitzen und meinen, dass die Daten bereits von ihrem Anbieter entfernt würden und zu eigenen Datenvermögen des Unternehmens geworden wären. Daher kommt es zu einer Reihe von Streitigkeiten über Rechte auf Geschäftsdaten (Du Zhenhua & Cha Hongwang 2016).

Unternehmen, die auf Geschäftsdaten angewiesen sind, verfügen in der Regel über große Datenmengen oder können diese massiv ansammeln. Sie sind jedoch möglicherweise nicht in der Lage, Wert oder innovative Gedanken aus Geschäftsdaten herauszuholen. Daher ist es notwendig und wichtig, einen reibungslosen Fluss von Geschäftsdaten zu ermöglichen, damit solche Ressourcen aus verschiedenen Blickwinkeln und auf verschiedenen Ebenen abgebaut und wiederholt verwendet werden können. Um dies zu erreichen, müssen wir eine gute Ordnung auf dem Datenmarkt sicherstellen, indem wir die Eigentumsrechte in Bezug auf Daten klar definieren und das Dateneigentum, d.h. „Daten mit ihrem Eigentümer“ klarstellen. Um den maximalen Datenwert zu erzielen, muss daher das Teilhaberecht an Geschäftsdaten festgelegt werden, um die Interessen verschiedener Beteiligten auszugleichen, ihre Ansprüche auf Interessen zu schützen und die breite Anwendung von Geschäftsdaten zu ermöglichen.

Das Teilhaberecht an Geschäftsdaten ist das Recht zur Teilhabe an Geschäftsdaten. In gewissem Sinne ist die Teilhabe an Geschäftsdaten ein anderer Name der Geschäftsdatentransaktionen. Das Teilhaberecht auf Geschäftsdaten wird daher auch als Handelsrecht auf Geschäftsdaten bezeichnet. Derzeit ist der Umfang der Geschäftsdaten relativ klein, kann

jedoch erweitert werden, indem öffentliche Daten durch Öffnung und persönliche Daten durch Teilhabe in einen Teil von Geschäftsdaten umgewandelt werden. Nur wenn Daten kommerziell genutzt werden, kann ihr Wert in höchstem Maße freigesetzt werden. Daher stellt die Kommerzialisierung der Geschäftsdaten den allgemeinen Trend dar und das Teilhaberecht auf Geschäftsdaten ist der vielversprechendste Teil des Datenteilhaberechts. Das Teilhaberecht an Geschäftsdaten erleichtert den freien Verkehr von Geschäftsdaten innerhalb der gesamten Gesellschaft, damit mehr Menschen Möglichkeit haben, Daten zu nutzen und so den Datenwert durch Teilhabe zu steigern.

3. Das Teilhaberecht auf personenbezogenen Daten

Menschen sind die primäre Datenquelle. Daher soll die Erforschung von Daten zum menschenorientierten Analyseparadigma zurückkehren. Bis zu einem gewissen Grad können alle Daten als personenbezogene Daten betrachtet werden. Die in den Daten enthaltenen persönlichen Informationen können sich auf eine bestimmte natürliche Person beziehen und sogar sensible persönliche Daten und Kernprivatsphäre betreffen. Wenn diese Daten nicht desensibilisiert oder nicht vollständig desensibilisiert sind, erhalten andere Personen möglicherweise die persönlichen Informationen und Privatsphäre aus den damit zusammenhängenden Daten, was zu einer Verletzung der persönlichen Datenrechte führen kann. Mit der Entwicklung der modernen Wissenschaft und Technologie wird die Erfassung und Übertragung von persönlichen Daten noch einfacher und effizienter. In gewissem Maße ist der Datenteilhabe eine Art und Weise, personenbezogene Daten zu sammeln, zu übertragen und wiederzuverwenden. Da Teilhabedaten viele personenbezogene Daten enthalten, soll das Teilhaberecht auf personenbezogenen Daten die gesetzmäßige Verarbeitung personenbezogener Daten als seine Voraussetzung haben.

Die Datenteilhabe bezieht sich auf personenbezogene Daten, es besteht jedoch ein Mangel an allseitigen Schutz für personenbezogene Daten in der Datenteilhabekette: Einerseits kann der Schutz personenbezogener Daten während der Datenerfassung, die den ersten Teil der Kette darstellt, aufgelöst werden, vor allem wegen unbegrenzter Ermächtigung,

was dazu führen kann, dass Eigentümer personenbezogener Daten in der Regel die Kontrolle über ihre personenbezogenen Daten verlieren, nachdem sie die Genehmigung zum ersten Mal erteilt haben. Daher ist es schwierig sicherzustellen, dass die personenbezogenen Daten so verwendet werden, wie sie beabsichtigt sind. Andererseits fehlt es an einem wirksamen Autorisierungsmechanismus, was die gewährende Seite ermöglicht, die Rechtmäßigkeit der Verwendung personenbezogener Daten infrage zu stellen, wodurch die Effizienz der Teilhabe personenbezogener Daten aber beeinträchtigt wird. Deshalb kann uns die Einrichtung des Teilhaberechts auf personenbezogenen Daten dabei helfen, die Rechte und Interessen im Zusammenhang mit der Teilhabe personenbezogener Daten auf wirksame und angemessene Weise zu schützen und zu verteilen. Das Teilhaberecht auf personenbezogenen Daten ist ein Recht, das Menschen ermutigt, mit Datensammlern zusammenzuarbeiten und mehr Daten zu produzieren. Es motiviert Menschen, Daten zu produzieren und damit die Gesellschaft ständig mit Daten zu versorgen. In diesem Sinne ist das Teilhaberecht auf personenbezogenen Daten der wichtigste Teil des Teilhaberechts.

Im Wesentlichen bedeutet die Teilhabe personenbezogener Daten, dass personenbezogene Daten von anderen Personen erneut gesammelt und verwendet werden. Daher hat das Teilhaberecht auf personenbezogenen Daten zwei Dimensionen: Erstens aus dem Blickwinkel der Sammler der persönlichen Daten versteht man unter dem Teilhaberecht auf personenbezogenen Daten tatsächlich das Recht, mit dem die Datensammler die von ihnen erfassten persönlichen Daten in Verkehr bringen; es ist möglich, dass sie gemeinsam mit spezifischen Subjekten diese persönlichen Daten gemeinsam nutzen, oder es ist auch möglich, dass sie diese persönlichen Daten für unbestimmte Subjekte offenlegen und in Umlauf bringen, damit mehr Subjekte über Daten verfügen. Zweitens aus Sicht derjenigen, deren Daten gemeinsam genutzt werden, können diejenigen, die die teilhabbaren persönlichen Daten erhalten, durch Teilhabe nicht nur diese Daten wiederverwenden, sondern diese auch verarbeiten, nutzen und sogar erneut daran teilhaben. Daher sollen Dateninhaber nicht die Möglichkeit haben, Daten willkürlich zur Teilhabe von anderen weiterzugeben, während diejenigen, die teilhabbaren Daten erhalten, weder nach Belieben weitergeben noch anderen erlauben dürfen, die von ihnen erfassten Daten zu verwenden

(Wang Liming 2019). Das Teilhaberecht auf personenbezogenen Daten soll die Dominanz des Einzelnen über Daten, die privatrechtliche Autonomie und die Menschenwürde bewahren. Das bedeutet, dass die Offenlegung und Teilhabe personenbezogener Daten unter der Voraussetzung gefördert werden soll, dass die Grundrechte des Einzelnen auf personenbezogenen Daten wirksam geschützt werden.

(II) Funktionen des Teilhaberechts

Das Teilhaberecht unterscheidet sich in engem Sinn und breitem Sinn. Im engen Sinne bezieht sich das Teilhaberecht auf das Recht, Daten mit anderen zu teilen; im weiten Sinne bezieht sich das Teilhaberecht auf Recht, das sich aus dem gesamten Lebenszyklus des Verhaltens beim Datenteilhaben ergeben. Hier verwenden wir den Begriff hauptsächlich im weiteren Sinne und das Teilhaberecht hat daher vier Rechtskompetenzen: das Zugriffsrecht auf Teilhabedaten, das Nutzungsrecht auf Teilhabedaten, das Ertragsrecht auf Teilhabedaten und das Verfügungsrecht auf Teilhabedaten. Das Zugriffsrecht auf Teilhabe ist das Recht, mit dem man Teilhabedaten beschaffen darf; das Nutzungsrecht auf Teilhabe ermöglicht Personen, an Daten teilzuhaben; das Ertragsrecht auf Teilhabe bedeutet das Recht, Einnahmen aus Teilhabedaten zu erzielen und das Verfügungsrecht über Teilhabedaten bedeutet, dass man das Recht hat, über Teilhabedaten zu verfügen. Die Daten hier umfassen sowohl Teilhabedaten als auch Originaldaten.

1. Das Zugriffsrecht auf Teilhabedaten

Der Zugriff auf teilhabbaren Daten ist eine grundlegende Datenaktivität. Nur wenn man Zugriff auf Daten hat, kann er die Kontrolle darüber übernehmen und wirklich an diese teilhaben. Das Recht auf Zugriff auf teilhabbaren Daten soll festgelegt werden, um sicherzustellen, dass das Recht auf Zugriff auf teilhabbaren Daten legitim und gerechtfertigt ist. Das sogenannte Zugriffsrecht auf Teilhabedaten bedeutet das Recht, mit dem man Teilhabedaten gesetzmäßig und ordnungsgemäß beschaffen kann.

Die Ausübung des Zugriffsrechts auf Teilhabedaten muss eingeschränkt und der Wille des Dateninhabers als Voraussetzung dafür genommen werden. Niemand darf beliebig Zugriff auf Daten haben, sonst würden schwere Fragen der Datensicherheit mit sich gebracht werden.

Subjekte des Zugriffsrechts auf Teilhabedaten können universal alle Bedarfsträger an Teilhabedaten sein, einschließlich natürlicher Personen, juristischer Personen und öffentlicher Einrichtungen usw. Das Recht auf Zugang zu Teilhabedaten in weitem Sinne ist sowohl ein Grundrecht der Bürger im Bereich des öffentlichen Rechts als auch ein wichtiges Zivilrecht im Bereich des Privatrechts. Aus Sicht des öffentlichen Rechts ist der freie Zugang zu Daten eine Voraussetzung für die politische Beteiligung und Diskussion der Bürger. Ohne das Recht auf Zugang zu Teilhabedaten können daher die Grundrechte der Bürger nicht garantiert werden. Der Staat als Subjekt des öffentlichen Rechts hat auch das Recht, auf Teilhabedaten zuzugreifen. Hätte der Staat keinen vollständigen Zugang zu Teilhabedaten, würde die politische, wirtschaftliche und kulturelle Entwicklung des Landes keine solide Grundlage haben. Aus privatrechtlicher Sicht ist das Recht auf Zugang zu Teilhabedaten ein grundlegendes Recht, mit dem Zivilsubjekte zivile Aktivitäten ausüben. Nur wenn Verbraucher ausreichend Zugang zu Warendaten haben, können Warentransaktionen fair und gerecht erfolgen. Ohne Garantie des Zugangsrechts zu Teilhabedaten könnte die Verwirklichung der Rechte und Interessen von Zivilsubjekten nur eine Fantasie sein. Das Zugriffsrecht auf Teilhabedaten ist eine Art Recht gegen Welt. Jede Organisation und jede Einzelperson soll seine Verwirklichung unterstützen (Zhou Shuyun 2014).

Das Objekt des Zugriffsrechts auf Teilhabedaten ist der Gegenstand, auf den es deutet und der die Interessen der Dateninhaber trägt und auf dem die Interessen der Dateninhaber stützt. Als Datenobjekt fallen die Teilhabedaten in verschiedene Typen mit jeweils unterschiedlichen Merkmalen. Vom Gesichtspunkt des Zugriffs auf Teilhabedaten aus können sie nach verschiedenen Klassifizierungskriterien in verschiedenen Typen eingeteilt werden. Im allgemeinen Sinne umfassen die Objekte des Zugangsrechts zu Teilhabedaten Datenressourcen, Datentechnologien, Datenkanäle und Datendienste usw. Oder im engeren Sinne sind die Objekte des Zugangsrechts zu

Teilhabedaten nur die Teilhabedaten, die die Eigenschaft wie Öffentlichkeit, Erneuerbarkeit, Aktualität, Wertigkeit und Knappheit usw. besitzen. Diese Merkmale sind Voraussetzung für die Errichtung des Zugriffsrechts auf Teilhabedaten. Nur wenn dieses Recht sichergestellt und geschützt ist, kann der Bedarf der Bürger an Zugang zu Teilhabedaten befriedigt und der Wert des Zugriffsrechts auf Teilhabedaten maximal verwirklicht werden (Zhou Shuyun & Wang Haoyun 2015).

Der Zugriff auf Teilhabedaten ist ein komplizierter Prozess. Der Inhalt des Rechts auf Zugang zu Teilhabedaten, d.h. was von den Bürgern wirklich erworben werden kann, ist die Interessen, die mit Kernelementen wie Datenressourcen, Datentechnologien, Datenkanälen und Datendiensten etc. verbunden sind. Daher enthält das Zugriffsrecht auf Teilhabedaten vier grundlegende Rechte: das Wahlrecht auf Inhalt der Teilhabedaten, das Auskunftsrecht auf Technologien für Teilhabedaten, das Kontaktrecht, auf Kommunikationskanälen für Teilhabedaten und das Recht auf garantierte Teilhabedaten-Servicequalität. Das Wahlrecht auf Inhalt der Teilhabedaten bedeutet, dass der Rechtsinhaber die Freiheit hat, den Inhalt der Teilhabedaten zu wählen. Das Auskunftsrecht auf Technologien für Teilhabedaten bedeutet, dass der Rechtsinhaber das Recht hat, sich über relevante Datenerfassungstechnologien informiert zu werden. Das Kontaktrecht auf Kommunikationskanäle für Teilhabedaten bedeutet, dass der Rechtsinhaber das Recht hat, zur Beschaffung von Teilhabedaten Kontakt mit Medien der Teilhabedaten zu nehmen; und das Recht auf garantierte Teilhabedaten-Servicequalität bedeutet, dass der Benutzer bei Verwendung von Teilhabedaten das Recht hat, relevante Dienstleister aufzufordern, qualitativ hochwertige, effiziente und faire Dienstleistung in Bezug auf Teilhabedaten bereitzustellen und eine relativ hohe Qualität der gelieferten Produktinhalte der Teilhabedaten sicherzustellen (Zhou Shuyun & Luo Xueying 2014).

2. Nutzungsrecht auf Teilhabedaten

Verwendung ist ein Mittel der Nutzung von Teilhabedaten und eine Weise für Ausgrabung des Werts von Teilhabedaten. Das Recht, Teilhabedaten zu verwenden, wird als Nutzungsrecht auf Teilhabedaten

bezeichnet. Der Zweck der Errichtung des Teilhaberechts liegt nicht darin, dass man Zugriff auf Teilhabedaten hat, sondern dass sie verwendet werden. Durch Teilhabe an Daten kann man Bedürfnisse des Rechtsinhabers erfüllen und so entsprechende Interessen erzielen. Daher ist es erforderlich, das Verwendungsrecht auf Teilhabedaten einzuführen. Dies wird durch den Nutzungswert der Teilhabedaten bestimmt. In der Zwischenzeit kann das Nutzungsrecht auf Teilhabedaten von den Teilhaberechten getrennt werden, um eine unabhängige Funktion zu schaffen und eine wichtige Grundlage für Begründung von Nießbrauchrecht auf Daten und Nießbrauchrecht auf öffentliche Daten zu bilden. Anders als das Nutzungsrecht im Sinne der herkömmlichen Rechtskunde muss das Nutzungsrecht auf Teilhabedaten in Übereinstimmung mit den Willen der Datenanbieter ausgeübt werden. Daher ist das Nutzungsrecht auf Teilhabedaten tatsächlich eine eingeschränkte Art des Nutzungsrechts. Das Nutzungsrecht auf Teilhabedaten ist das Recht, das den Nutzungswert von Daten verfolgt und durch Datennutzung entsprechende Interessen erlangt. Es umfasst hauptsächlich zwei Arten wie Verarbeitungsrecht und Reproduktionsrecht auf Teilhabedaten. Die Verarbeitung ist eine grundlegende Methode für Verwendung der Teilhabedaten. Durch Datenverarbeitung kann der Wert der Teilhabedaten festgestellt und aufgewertet werden. Daher ist das Verarbeitungsrecht auf Teilhabedaten ein wichtiger Bestandteil des Nutzungsrechts auf Teilhabedaten. Man kann auch am Verarbeitungsrecht auf Teilhabedaten teilhaben. Solche Teilhabe ist üblicherweise bedingt, d.h. diejenigen, die dieses Recht aufgrund der Freigabe erhalten, dürfen die Daten jedoch nur auf die vereinbarte Weise verarbeiten. Um den Wert von Teilhabedaten zu vermehren, muss der Umfang der Teilhabedaten jedoch vergrößert werden, damit mehr Kunden diese Daten verwenden können. Da die Kosten extrem niedrig sind, ist die Datenkopierung zu einem wichtigsten Mittel dafür geworden. Das Reproduktionsrecht auf Teilhabedaten spielt daher eine wichtige Rolle im Nutzungsrecht auf Teilhabedaten. Das ist eine wichtige Bedingung für die Verwendung von Teilhabedaten und gewährleistet die vollständige Wiedergabe der in den Daten enthaltenen Informationen (Schlüssel-Labor der Big-Data-Strategie 2018, S. 195).

3. Ertragsrecht auf Teilhabedaten

Das sogenannte Ertragsrecht auf Teilhabedaten bezieht sich auf das Recht, mit Teilhabedaten Einnahmen zu erzielen. Nach dem Zugriff auf Teilhabedaten kann man nicht nur diese verwenden, sondern auch einige Einnahmen daraus erzielen. Da diese Einnahmen aus den Teilhabedaten abgeleitet werden, wird das Ertragsrecht auf Teilhabedaten auch als Recht bezeichnet, natürliche und gesetzmäßige Vermehrzinsen aus Teilhabedaten zu erhalten. In der modernen Gesellschaftsform ist eine bedeutende Tendenz der Entwicklung von Rechten die Verlagerung von abstrakter Herrschaft zu konkreter Nutzung. Die Einrichtung des Ertragsrechts auf Teilhabedaten entspricht der Tendenz der Entwicklung des Zeitalters und ermöglicht die Trennung der Teilhaberechte. Das Ertragsrecht auf Teilhabedaten unterliegt jedoch Einschränkungen von Rechtsobjekten. Während der Zweck der Datentransaktion darin besteht, Erträge aus Teilhabedaten zu erzielen, spielt das Ertragsrecht auf Teilhabedaten eine wichtige Rolle bei der Erweiterung des Umfangs der Datentransaktion und der Festlegung der Ordnung für Datentransaktionen. Die Kapitalisierung von Teilhabedaten ist in der Tat ein Prozess der Erlangung von Ertragsrechts sowie eine Form, in der das Ertragsrecht auf Teilhabedaten in wirtschaftlicher Hinsicht realisiert wird. Die Teilhabedaten können ihren Wert nur mit dem Ertragsrecht auf Teilhabedaten realisieren und so weisen die Merkmale wie Äußerlichkeit, Langfristigkeit und Pluralität etc. aus. Die Äußerlichkeit bedeutet das Verhältnis der Einnahmen aus der Nutzung von Teilhabedaten zu den gezahlten Kosten vom Inhaber des Ertragsrechts auf Teilhabedaten. Sie bestimmt die Nichtabsolutheit der Teilhabedaten. Deshalb sollen dem Ertragsrecht auf Teilhabedaten notwendige Beschränkungen auferlegt werden, um ein Gleichgewicht zwischen privaten und öffentlichen Interessen herzustellen. Die Einnahmen aus Teilhabedaten haben die Eigenschaft der Langfristigkeit, da der Wert der Teilhabedaten nicht durch einmalige Verwendung oder Verbrauch völlig ausgegraben werden kann. Wenn neue Datenressourcen hinzugefügt und mit dem verbunden werden, was bereits vorhanden ist, vermehrt der Wert der Teilhabedaten und neue Einnahmen werden

mitgebracht. Zugleich sind die Teilhabedaten nicht abnutzbar. Sie können umfangreicher geteilt und immer wieder verwendet werden, was über einen langen Zeitraum zu Renditen führt. Der Wert von Teilhabedaten kann niemals sein Maximum erreichen. Stattdessen kann er sich mit der Zeit ansammeln und ständig erweitern. Die Einnahmen aus den Teilhabedaten weisen eine Art von Vielfältigkeit auf, da es unmöglich ist, die Kontrolle über diese Daten vollständig zu übertragen, weil Daten nicht im absoluten Sinne ausgeliefert werden können. Es kann mehrere Subjekte der Ertragsrechte auf die gleichen Daten geben, die Erträge aus derselben Gruppe von Teilhabedaten erzielen (Schlüssel-Labor der Big-Data-Strategie 2018, S. 196).

4. Das Verfügungsrecht auf Teilhabedaten

Die Disposition bedeutet ultimative Verfügung über Daten. Das Recht zur Verfügung über Teilhabedaten ist das Recht, über Teilhabedaten zu verfügen. Aus einer anderen Perspektive kann Disposition als Endnutzung von Daten angesehen werden. Daher ist das Recht zur Verfügung über Teilhabedaten das Recht, die Teilhabedaten von Rechtsinhaber zu konsumieren und teilzuhaben, was die endgültige Manifestation der Teilhaberechte darstellt. Das Verfügungsrecht auf Teilhabedaten kann nicht dazu führen, dass die Anbieter der Teilhabedaten das Kontrollrecht über ihre Daten verlieren. Es ist vielmehr ein unabhängiger Teil der durch Datenreproduktion entstandenen Teilhaberechte, der es mehreren Inhabern der Teilhaberechte ermöglicht, gleichzeitig auf dieselben Daten zuzugreifen und diese zu verwenden. Das Verfügungsrecht auf Teilhabedaten kann den ursprünglichen Wert der Teilhabedaten nicht vernichten. Im Gegenteil erhöht es den Teilhabewert. Für physische Objekte führt die Disposition zum absoluten oder relativen Vernichten ihres Eigentumsrechts, das Recht zur Disposition bestimmt hier das Eigentumsrecht des physischen Objekts (Lu Xiaohua 2009, S. 373). Für Daten hingegen gilt das traditionelle Verfügungsrecht nicht mehr für den Schutz und die Nutzung der Teilhabedaten. Der Datenbesitz entspricht dem Entwicklungstrend von Daten nicht mehr. Da der Wert von Daten liegt in der Teilhabe. Kontrolle über Daten ist nicht der Zweck der Begründung

der Teilhaberechte. Nur wenn der Datenumfang vergrößert wird, können mehr Menschen die Möglichkeit haben, Daten zu nutzen und erst dann kann das Problem der Datenknappheit gelöst und der Wert der Daten voll ausgeschöpft werden. Das Verfügungsrecht auf Teilhabedaten bezieht sich vielmehr auf die Verwendung der Teilhabedaten, mit dessen Hilfe man durch Nutzung von Teilhabedaten den Wert von Daten verfolgen kann. Daher ist das Verfügungsrecht auf Teilhabedaten auf eine ebenso wichtige Position wie die des Eigentumsrechts auf Teilhabedaten gesteigert.

(III) „Nießnutzrecht auf persönlichen Daten“ und „Nießnutzrecht auf öffentlichen Daten“

Die Festlegung der Teilhaberechte ermöglicht die gemeinsame Nutzung von Daten zwischen verschiedenen Subjekten und führt zwangsläufig zu Konflikten zwischen Dateneigentum und Datennutzung. Um diese Konflikte zu lösen, schlagen wir den Begriff wie das „Nießnutzrecht auf persönlichen Daten“ und das „Nießnutzrecht auf öffentlichen Daten“ vor. Beide sind eingeschränkte Teilhaberechte und auch eine realistische Wahl für Verwirklichung der Teilhaberechte. Die Errichtung der beiden Rechte ermöglicht es, das Dateneigentumsrecht vom Datennutzungsrecht zu trennen. Das Nießnutzrecht auf Daten bezieht sich auf das Recht, Daten anderer Personen unter bestimmten Bedingungen zu verwenden und Einnahmen daraus zu erzielen, was dazu beiträgt, den Wert der Teilhaberechte zu verwirklichen und ist auch eine wichtige Methode für Realisierung der Teilhaberechte. Das Nießnutzrecht auf öffentlichen Daten ist eine Art übertragenes Nießnutzrecht auf persönlichen Daten. Es bezieht sich auf das Recht der von der Regierung vertretenen Verwaltungssubjekte sowie der öffentlichen Institutionen und Körperschaften von öffentlichen Interessen usw., ausgehend von Bedürfnissen der öffentlichen Interessen auf Daten für öffentliche Interessen zuzugreifen, diese zu verwalten, zu verwenden und teilzuhaben.

I. Nießnutzrecht auf persönlichen Daten

Das Nießbrauchrecht auf Daten bezieht sich auf das Recht, Teilhabedaten zu nutzen und dabei zu profitieren. Das bedeutet, dass der Rechtsinhaber andere zur Nutzung von Daten berechtigt. Das Nießbrauchrecht auf Daten wird eingeführt, um den Konflikt zwischen dem Eigentum und der Nutzung von Teilhabedaten beizulegen, und es ermöglicht Menschen, Teilhabedaten unter bestimmten Bedingungen zu nutzen und Einnahmen davon zu erzielen. Die Einführung des Nießbrauchrechts auf Daten ist ein Produkt des Übergangs der Datenrechte von der Kontrolle zur Nutzung und trägt dazu bei, den Wert der Teilhaberechte zu verwirklichen. Es ist eine Realisierungsform der Teilhaberechte. Die Entstehung des Nießbrauchrechts auf Daten ist auch ein Erfolg der Trennung der Funktionen der Teilhaberechte. Es handelt sich um eine Art von Datenrecht, das auf der Grundlage gebildet wird, dass ein Datenrechtsinhaber einige Funktionen seiner Teilhaberechte abtrennt und mit anderen teilt, so dass er ein Recht auf Daten anderer Personen hat. Daher hat das Nießbrauchrecht auf Daten auf Grundlage des Teilhaberechts entstanden und seine Existenz an sich stellt eine Einschränkung des Teilhaberechts dar. Die Einrichtung des Nießbrauchrechts auf Daten erfolgt häufig aus dem Willen des Datenrechtsinhabers, der unter den Umständen, dass er den Wert von Daten nicht tatsächlich nutzen oder in vollem Umfang nutzen kann, seine Daten mit anderen teilt, damit sie diese verwenden und Einnahmen daraus erhalten und den Wert der Daten vollständig ausgraben können. Mit dem Beginn des Zeitalters der digitalen Zivilisation erweitert sich der Umfang der Datenressourcen stets und das Nießbrauchrecht auf Daten gewinnt immer Wichtigkeit.

Da das Nießbrauchrecht an Daten auf Teilhabedaten basiert, das dem Fremdeigentumsrecht ähnlich ist, kann das Nießbrauchrecht an Daten als Fremdeigentumsrecht bezeichnet werden. Da das Nießbrauchrecht auf Daten nur innerhalb eines vereinbarten Umfangs über die betreffenden Daten verfügen muss, spricht man auch von einem beschränkten Datenrecht. Da die Subjekte des Nießbrauchrechts auf Daten andere Subjekte außer den Datenrechtsinhabern sind, können die Dateneigentumsinhaber nicht zu Subjekten des Nießbrauchrechts auf Daten werden. Weil

das Nießbrauchrecht auf Teilhabedaten beruht, so sind die Subjekte des Nießbrauchrechts auf Daten natürliche Personen, juristische Personen oder andere Organisationen, die Rechte auf Teilhabedaten haben. Weil es sich bei dem Gegenstand des Nießbrauchrechts um die Teilhabedaten handelt, die Merkmale wie Immaterialität, Reproduzierbarkeit und Nicht-Absolute-Ablieferbarkeit usw. aufweisen und durch die Diversifizierung der Art und Weise, wie man Daten verwendet, insbesondere Fortschritte in Wissenschaft und Technologie sowie Innovationen bei Systemen und Mechanismen, vermehrt sich der Wert der Teilhabedaten kontinuierlich. Um Teilhabedaten effizienter zu nutzen, ist es daher erforderlich, das Nießbrauchrecht auf Teilhabedaten einzuführen. Das ist ein unwiderstehlicher Trend der Entwicklung von Datenrechten.

Das Nießbrauchrecht an Daten ist das Recht, über den Nutzungswert der Teilhabedaten zu verfügen. Gesetzlich gesehen besteht der Hauptinhalt des Nießbrauchrechts auf Daten darin, Teilhabedaten zu nutzen und daraus zu profitieren. Daher umfasst der Inhalt des Nießbrauchrechts auf Daten das Zugangsrecht zu Teilhabedaten, das Nutzungsrecht auf Teilhabedaten und das Ertragsrecht auf Teilhabedaten. Einerseits ist es für die Nutzung von Daten erforderlich, auf Teilhabedaten zuzugreifen. Ohne das Zugriffsrecht können Nießbrauchrechtinhaber möglicherweise die Teilhabedaten nicht tatsächlich nutzen. Da das Nießbrauchrecht auf Daten die Teilhabedaten verwenden und daraus profitieren soll, um den Nutzungswert aus Daten herauszuholen, ist es erforderlich, dass der Rechtsinhaber Zugriff auf die Zieldaten erhält. Das Zugriffsrecht auf Teilhabedaten steht normalerweise im Mittelpunkt von Konflikten um Nießbrauchrecht auf Daten, da der Zugriff als Voraussetzung für das Nießbrauchrecht an Daten festgelegt worden ist. Nur wenn der Nießbrauchrechtinhaber auf Daten Teilhabedaten erhält, kann die Nutzung und Profitierung von Daten verwirklicht werden und dann der Nutzungswert der Daten erzielt werden. Andererseits nimmt das Nießbrauchdatenrecht Nutzung von Teilhabedaten und Erlöse daraus als sein Ziel. Unter dem Nutzungsrecht auf Teilhabedaten wird das Recht verstanden, mit dem die Teilhabedaten gemäß der Art und dem Zweck der Teilhabedaten auf der Grundlage von Gesetzen oder einschlägigen Vereinbarungen zu nutzen. Der Zweck für die Einrichtung des Nießbrauchdatenrechts besteht darin, Teilhabedaten

besser zu nutzen und mehr Nutzungswert daraus zu ziehen. Aus Teilhabedaten zu verdienen bedeutet, durch erhaltene Teilhabedaten natürliche und gesetzmäßige Mehrzinsen zu gewinnen. Die Nutzung und Einnahmen sind in der Regel eng miteinander verbunden, da man nur nach Verwendung der Teilhabedaten Einnahmen daraus erzielen kann. Daher soll das Nießbrauchdatenrecht sowohl das Nutzungsrecht auf Teilhabedaten als auch das Ertragsrecht auf Teilhabedaten umfassen. Dies liegt daran, dass die direkte Bedeutung des Nießbrauchdatenrechts im Rechtsbereich das Nutzungsrecht ist. Dabei handelt es sich um eine Art Datenrecht, das die Teilhabedaten zum Zwecke der Nutzung nutzt. Zugleich handelt es sich beim Nießbrauchdatenrecht um Nutzung des Nutzungswerts der Daten, um ihre unterschiedlichen Interessenbedürfnisse der Subjekte des Nießbrauchdatenrechts durch Nutzung zu erfüllen. In diesem Sinne umfasst das Nießbrauchdatenrecht auch Ertragsrecht auf Teilhabedaten (Schlüssel-Labor der Big-Data-Strategie 2018, S. 203).

2. Nießbrauchrecht auf öffentlichen Daten

Aus Sicht des privaten Rechts betont das Nießbrauchdatenrecht vor allem das Recht auf Nutzung und Einkommen aus Daten. Als das Gegenteil des Nießbrauchdatenrechts bezieht sich das Nießbrauchrecht auf öffentlichen Daten auf das Recht der von der Regierung vertretenen Verwaltungsbehörden sowie der öffentlichen Institutionen und Organisationen von öffentlichen Interessen, auf Gemeinnutzdaten zuzugreifen, diese zu verwalten, zu verwenden und zu verfügen. Das Nießbrauchrecht auf öffentliche Daten ist gesetzlich gesehen eine Art übertragenes Nießbrauchdatenrecht und ein Grunddatenrecht der Bürger. Es handelt sich um einen neuen Anspruch auf Datenrechte, die gemeinnützig sind und für öffentliche Versorgungsunternehmen, öffentliche Dienste und öffentliche Verwaltung verwendet werden. Das Nießbrauchrecht auf öffentliche Daten ist volkseigen. Die Von der Regierung vertretenen Verwaltungsbehörden, öffentlichen Institutionen und öffentliche Wohlfahrtsorganisationen werden nur aus Bedürfnissen der öffentlichen Interessen dieses Recht vertretungsweise beherrschen. Die Wahrung der öffentlichen Interessen ist der grundlegende Zweck des Nießbrauchrechts auf öffentliche

Daten und auch ein scharfes Schwert für wirksame Einschränkung der privaten Rechte (Schlüssel-Labor der Big-Data-Strategie 2018, S. 212).

Ausgehend von der Wahrung der öffentlichen Interessen soll das Nießbrauchrecht auf öffentliche Daten folgende Funktionen umfassen: das Zugangsrecht, das Verwaltungsrecht, das Nutzungsrecht und das Verfügungsrecht. Obwohl die Öffentlichkeit durch Verwendung von Gemeinnutzdaten entsprechende Einnahmen erzielen kann, umfasst das Nießbrauchrecht auf öffentlichen Daten an sich nicht die Funktion für Ertrag. Dies liegt daran, dass es sich bei der Verwendung von Gemeinnutzdaten durch die Öffentlichkeit dem Wesen nach um Ausübung des Nießbrauchdatenrechts auf Gemeinnutzdaten aber nicht um Ausübung des Nießbrauchrechts auf öffentliche Daten. Nur die Verwaltungsbehörden, öffentlichen Einrichtungen und Gemeinwohlkörperschaften als Vertreter der Öffentlichkeit können berechtigt werden, das Nießbrauchrecht auf öffentlichen Daten auszuüben. Und während der Ausübung des Nießbrauchrechts auf öffentlichen Daten dürfen sie keine Einnahmen aus öffentlichen Daten erzielen. Daher beinhaltet das Nießbrauchrecht auf öffentlichen Daten nicht die Funktion des Einkommens.

Das Zugangsrecht auf Gemeinnutzdaten bezieht sich auf das Recht der von der Regierung vertretenen Verwaltungsstellen, öffentlichen Institutionen und gemeinnützigen Organisationen gemäß den einschlägigen gesetzlichen Bestimmungen rechtzeitig, genau und ganzheitlich auf alle Arten von benötigten Gemeinnutzdaten auf bestimmte Art und Weise zuzugreifen. Natürlich muss die Ausübung des Zugangsrechts auf Gemeinnutzdaten eingeschränkt werden, da sonst die Rechte auf öffentlichen Daten unbegrenzt erweitert würden. Das Verwaltungsrecht auf Gemeinnutzdaten bezieht sich auf das Verwaltungsrecht, das von den durch Regierung vertretenen Verwaltungsbehörden, öffentlichen Institutionen und gemeinnützigen Organisationen auf Gemeinnutzdaten ausgeübt wird, um die Zwecke der öffentlichen Nutzung von Gemeinnutzdaten zu erreichen. Aus Sicht der Rechtsnatur ist das Verwaltungsrecht auf Gemeinnutzdaten eine gesetzliche Verpflichtung, da es die Verwaltungsmacht der von der Regierung vertretenen Verwaltungsbehörden, öffentlichen Institutionen und gemeinnützigen Organisationen ist, um öffentliche Interessen zu gewährleisten und zu stärken und Verwaltungspflichten zu

erfüllen. Das Nießbrauchrecht auf öffentliche Daten ist daher eine Art Verwaltungsbefugnis, die im öffentlichen Recht verbindlich ist. Zugleich kann das Verwaltungsrecht auf Gemeinnutzdaten dazu beitragen, das Recht der Bürger zu gewährleisten, Gemeinnutzdaten zu verwenden und willkürliches Verhalten von Verwaltungsstellen zu beschränken. Das Nutzungsrecht auf Gemeinnutzdaten ist der Kern des Nießbrauchrechts von öffentlichen Daten und dient dazu, Gemeinnutzdaten öffentlich zu nutzen und öffentliche Interessen sicherzustellen und zu erhöhen. Das Nutzungsrecht auf Gemeinnutzdaten bezieht sich daher auf das Recht der von der Regierung vertretenen Verwaltungsbehörden, öffentlichen Institutionen und gemeinnützigen Organisationen, Daten von öffentlichen Interessen zu verwenden. Das Verfügungsrecht auf Gemeinnutzdaten bezieht sich auf das Recht der von der Regierung vertretenen Verwaltungsbehörden, öffentlichen Institutionen und gemeinnützigen Organisationen die von ihnen verwalteten Gemeinnutzdaten in ihrer Verantwortung mit anderen zu teilen. Es kann in zwei Arten unterteilt werden: Die eine ist das Recht auf Disposition von Gemeinnutzdaten im engeren Sinne, das sich auf Teilhabe an Gemeinnutzdaten zwischen verschiedenen Verwaltungsorganen bezieht. Nach der Teilhabe bleiben sie weiterhin Gemeinnutzdaten. Die Verwaltungsorgane, die Gemeinnutzdaten erhalten, genießen einen Teil der Funktionen des Nießbrauchrechts auf diese öffentlichen Daten und können diese Daten verwenden und verwalten. Die andere ist das Recht, Zugang zu Gemeinnutzdaten zu gewähren, was sich auf das Recht von Verwaltungsorganen bezieht, die von ihnen verwalteten Gemeinnutzdaten für Unternehmen und einzelne Bürger offen zugänglich zu machen. Nachdem Unternehmen und einzelne Bürger das Kontrollrecht über Gemeinnutzdaten erlangt haben, wandeln sich diese Daten in Nießbrauchsdaten um und können somit zur Erzielung von Einnahmen verwendet werden.

Abschnitt IV Wert der Teilhaberechte

Aus Sicht der Gerechtigkeit handelt es sich bei den Teilhaberechten um öffentliche Rechte, die auf der Grundlage von Altruismus festgelegt

wurden. Es wird unweigerlich mit den bestehenden individuellen Rechten auf der Grundlage von Egoismus in Konflikt geraten und somit die kontinuierliche Verbesserung des Rechtssystems fördern. Aus Sicht der Ordnung werden die Teilhaberechte sicherlich die Regeln der Öffnung der Datenteilhabe verändern und neu gestalten, den freien und geordneten Verkehr von Datenressourcen fördern und zum Aufbau einer neuen Sozialordnung der Teilhabe beitragen. Aus wirtschaftlicher Sicht ist die Theorie über Wert der Teilhabe eine wichtige theoretische Entdeckung auf dem Gebiet der Ökonomie und wird unweigerlich die derzeitige Basis des wirtschaftlichen Wertes wieder aufbauen. Der Vorschlag für Teilhaberecht wird sicherlich neue Impulse für die wirtschaftliche Entwicklung geben und als wichtige Eckpfeiler für Erstellung der Regeln der digitalen Wirtschaft dienen.

(1) Der Gerechtigkeitswert der Teilhaberechte

Das Verhältnis zwischen privaten Rechten und öffentlichen Rechten ist widersprüchlich: Das Erste behauptet die Vorherrschaft privater Rechte, wonach niemand als Mittel zur Erlangung von Interessen für andere angesehen werden kann und dass individuelle Rechte den allgemeinen Interessen der Gesellschaft überlegen sind. Das Letztere befürwortet dagegen, Einzelpersonen als Mittel für bestimmte Zwecke zu nehmen, wobei jegliches Verhalten, Gesetz und jede Politik anhand des Kriteriums der Maximierung öffentlicher Interessen zu bewerten und zu prüfen sind. Seit dem Zeitalter der Aufklärung war die Betonung der Persönlichkeitsrechte in der westlichen Gesellschaft immer der Mainstream. Im Westen ist die Ansicht weit verbreitet, dass die Existenz der Gesellschaft und Regierung zum Schutz der privaten Rechte dient und dass die Verfolgung öffentlicher Interessen der Gesellschaft nicht auf Kosten der privaten Rechte erreicht werden kann. Der Standpunkt, der den öffentlichen Rechten Vorrang einräumt, hat jedoch auch erheblichen Einfluss. Es verfolgt eher die Interessen der Mehrheit als die der Minderheit. Eine gerechte Gesellschaft soll der Mehrheit ermöglichen, größere Interessen zu erhalten und das maximale Nettoguthaben zu erhöhen, selbst wenn dies auf Kosten

der Interessen der Minderheit erfolgt, die möglicherweise benachteiligt werden könnten. Daher gibt es natürliche Konflikte zwischen privaten und öffentlichen Rechten, wobei der größte Unterschied darin besteht, ob Recht als ein unabhängiges Element betrachtet wird. Die Ansicht des öffentlichen Rechts betrachtet das Recht eher als eine Funktion aber nicht als eine Variable zur Verwirklichung des totalen gesellschaftlichen Nutzens. Umgekehrt nimmt der Standpunkt der privaten Rechte den Einzelnen in den Mittelpunkt und glaubt, dass jeder Einzelne der beste Richter über seine eigenen Interessen und deren Förderer ist, wobei die ganzheitlichen utilitaristischen Interessen der Gesellschaft und jede Form der Kontrolle des Einzelnen die privaten Rechte nicht ersetzen oder sogar unterdrücken können (Dong Yurong 2010).

Die Theorie der privaten Rechte und die Theorie der öffentlichen Rechte erklären jeweils ihre Grundkonzepte aus den Perspektiven des Egoismus und des Altruismus. Beide sind einzelne Wertauswahl. In der komplizierten realen Welt ist eine solche einseitige Denkweise in der Regel zu einfach, um eine Verallgemeinerung vorzunehmen, was auch der Hauptgrund ist, warum beide Theorien ihre Grenzen haben. Private Rechte implizieren das Prinzip der Staatsneutralität,⁴ das die positive Funktion des Staates ignoriert. Einige Wissenschaftler glauben, dass nur Einzelpersonen das Recht haben, Selbstwert und Selbstgüte anzustreben, während der Staat das Streben der Einzelnen nach Selbstwert nur im schwächsten Sinne schützt (Dong Yurong 2010). Sie sieht nur das „persönliche Güte“, nicht aber das „grundlegende soziale Güte“, das der Staat wahren sollte, und ignoriert somit die positive Funktion des Staates. Darüber hinaus trennen private Rechte die Verbindungen zwischen Gesellschaft und Individuum und tragen wenig zur Verwirklichung des Selbstwertgefühls bei. Private Rechte betonen die Priorität des Einzelnen in der Ontologie und sind der Ansicht, dass die Gesellschaft oder der Staat nur als Instrument

4 Staatsneutralität bedeutet, dass der Staat nichts mit Güte und Werten zu tun hat. Der britische Gelehrte Joseph Raz schrieb in *The „Morality of Freedom“*: „Regierungen müssen neutral gegenüber den Vorstellungen der verschiedenen Menschen vom Guten und von gutem Leben sein. Das heißt, die Regierungen müssen sich so verhalten, dass ihre Handlungen die Chancen des Einzelnen, im Einklang mit seiner Vorstellung vom Guten zu leben, weder verbessern noch behindern.“

zur Verwirklichung des persönlichen Ziels des rationalen Eigeninteresses dienen. Daher verleiht der Liberalismus dem Einzelnen aus Sicht der privaten Rechte das höchste Recht und betrachtet die privaten Rechte als überlegen über den öffentlichen Interessen der Gesellschaft.

Das größte Problem im Bereich der öffentlichen Rechte ist die Vernachlässigung der Grundrechte. Der Zweck der öffentlichen Rechte besteht darin, öffentliche Interessen zu maximieren, indem die Übertragung der persönlichen Interessen einiger Menschen erfordert wird, damit andere Menschen vergleichsweise mehr Interessen erhalten und die Gesamtinteressen der Gesellschaft zunehmen können. Der Standpunkt, der die öffentlichen Rechte betont, ist der Ansicht, dass sich eine solche Übertragung lohnt und die daraus resultierende Ungleichheit gerechtfertigt ist. Dieser Ansatz sorgt eher für die Zunahme der öffentlichen Gesamtinteressen der Gesellschaft als die Verteilung dieser Interessen unter den Menschen. Seit Langem hat man immer daran gezweifelt, ob öffentliche Rechte öffentliche Interessen quantifizieren können. Weil die öffentlichen Rechte öffentliche Interessen normalerweise mit Intuition messen und das Problem, dass unterschiedliche Menschen unterschiedliche Wahrnehmungen haben, nie vermeiden konnten. Daher ist es sehr schwierig, öffentliche Interessen rein objektiv zu berechnen (Dong Yurong 2010).

Die Konflikte zwischen privaten und öffentlichen Rechten sind die unvermeidlichen Folgen der Entwicklung der Gesellschaft und können mit dem Teilhaberecht beigelegt werden. Erstens drängen die Teilhaberechte private Rechte aus dem privaten Bereich in den öffentlichen Bereich. Das Individuum existiert nicht wie Atom isoliert, sondern als Teil des Systems der sozialen Zusammenarbeit. Das Teilhaberecht ermöglicht es den Menschen, durch Zusammenarbeit voneinander zu profitieren, dadurch die Gerechtigkeit garantiert wird. Das logische Ergebnis der Teilhaberechte ist daher eine erhöhte Aufmerksamkeit für den Wert der Gleichheit und für die privaten Rechte im öffentlichen Leben, was sicherlich gerecht ist. Zweitens nehmen die Teilhaberechte Anpassungen an der Gesamtheit der öffentlichen Rechte vor. Wenn öffentliche Rechte das Interesse für die Gesellschaft als Ganzes verfolgen, könnten sie für einige Menschen zum Verlust von Interessen führen. Als Reaktion darauf können die Teilhaberechte die ungleiche Verteilung anpassen, damit sie für den gegenseitigen Nutzen

gut geeignet sind. Durch Vermeidung zufälliger Faktoren im natürlichen und sozialen Umfeld in der Struktur von Gleichheit und Freiheit kann man die Gerechtigkeit des gegenseitigen Respekts in der sozialen Struktur zeigen. Das erfordert, dass man einander als Zweck und nicht als Mittel betrachten soll. Das Teilhaberecht garantiert daher die Wirksamkeit und Harmonie der sozialen Zusammenarbeit zwischen Menschen auf der Grundlage des Selbstwertgefühls und des gegenseitigen Nutzens und verhindert Verletzungen der Rechte einiger Menschen, die sich aus der Gesamtheit der öffentlichen Rechte ergeben. Schließlich kann das Teilhaberecht die durch öffentliche Rechte verursachte Ungerechtigkeit verhindern. Das Teilhaberecht betont, dass die Verteilung des sozialen Reichtums für alle in der Gesellschaft, insbesondere für die benachteiligten Gruppen günstig ist, und behebt damit das Problem, dass die öffentlichen Rechte die persönlichen Entscheidungen einfach auf diejenigen beschränken, die die öffentlichen Interessen maximieren. Darüber hinaus lösen die Teilhaberechte auch das Problem der Zufälligkeit im Utilitarismus. Weil Menschen von Natur aus durch Unterschiede in der natürlichen Ausstattung und Eignung ungleich gemacht worden sind, können die Teilhaberechte solche Unterschiede der natürlichen Veranlagung mit institutionellen Vereinbarungen ausgleichen. So können Teilhaberechte die sozialen Unterschiede und Unterschiede der natürlichen Anlagen beseitigen und damit dazu beitragen, Gerechtigkeit im eigentlichen Sinne zu erreichen.

(II) Ordnungswert der Teilhaberechte

Die sogenannte Ordnung der Teilhaberechte bezieht sich auf die Art der sozialen Ordnung, die die Teilhabe als ihren grundlegenden Anspruch betrachtet. Die Ordnung der Teilhabe im weiteren Sinne besteht seit der Geburt der menschlichen Zivilisation. Sprachen in ihrer mündlichen und schriftlichen Form sind Kanäle für Teilhabe, während Arbeitsteilung, Zusammenarbeit und Warentransaktion die Mittel zur Teilhabe darstellen. Das Alles war schon immer Teil der menschlichen Zivilisation. Teilhabe dient als Ziel und Richtung der Entwicklung der menschlichen Gesellschaft. Da die Teilhaberechte allmählich Wurzeln tief in den

Herzen der Menschen schlagen, ist die Ordnung der Teilhabe wieder in den Mittelpunkt der Entwicklung der menschlichen Zivilisation gerückt.

Das Teilhaberecht verändert die institutionellen Arrangements der Gesellschaft. Aus der Perspektive der sozialen Gerechtigkeit zeigen die substantielle und institutionelle Gerechtigkeit der Teilhabe eine sich gegenseitig verstärkende Beziehung. Einerseits ist die substantielle Gerechtigkeit der Teilhabe die Grundlage der institutionellen Gerechtigkeit. Die Kriterien für Beurteilung, ob das Teilhabesystem gerecht ist, müssen so sein, ob es die Entwicklung von Produktivkräften fördert und ob es mit der Produktionsweise übereinstimmt. Andererseits ist die institutionelle Gerechtigkeit der Teilhabe die Garantie für substantielle Gerechtigkeit, die Konkretisierung und Materialisierung des Wertes der Gerechtigkeit und die institutionelle Garantie für Verwirklichung substantieller Gerechtigkeit (Miao Ruidan & Dai Junyuan 2017). Daher ist es notwendig, die Ausübung der Teilhaberechte durch den Aufbau eines Teilhabesystems zu gewährleisten. Dieses System muss ein gutes Verhältnis zwischen Wirtschaft und Gesellschaft aufrechterhalten, da die Wirtschaft Effizienz als ihr Kernziel anstrebt, um mehr materiellen Wohlstand zu schaffen, während die Gesellschaft Fairness als ihr Kernziel anstrebt, damit mehr Menschen vom materiellen Wohlstand profitieren können. Bis zu einem gewissen Grad ist das Verhältnis zwischen der Teilhabewirtschaft und Teilhabegesellschaft widersprüchlich, und eine Anpassung durch ein solides Teilhabesystem ermöglicht beiden, ihre Rollen besser zu spielen. Das Teilhaberecht ist das Ergebnis des Arrangements durch das Teilhabesystem, die ein Gleichgewicht zwischen Effizienz und Gerechtigkeit darstellen.

Das Teilhaberecht optimiert die Datenhierarchie. Die sogenannte Datenhierarchie bezieht sich auf die Schichtungsstruktur, die sich aus Statusunterschieden der Daten ergibt. In dieser Datenhierarchie werden verschiedene Statusschichten nicht nur aus Berufsunterschied gebildet, sondern auch Schichten auf der Grundlage von Faktoren wie der Datenkapazität und dem Volumen der Datenressourcen, über die man verfügt, entstehen. Es gibt tendenziell klare Differenzierungslinien zwischen Menschen der verschiedenen Datenschichten und die Trends der Schichtung, Hierarchie und Verfestigung sind in der Datenstruktur immer klarer. Wenn die Liquidität von Faktoren wie Datentechnologien, Datenkapital und

Datenressourcen nicht ausreichend ist, werden sich verschiedene Faktoren tendenziell stets auf die höheren Schichten konzentrieren, während die Faktoren in den niedrigeren Schichten wenig Gewinngefühl haben. Dies führt zu einem Ungleichgewicht beim Besitz und Verteilungsverhältnis der Datenressourcen auf verschiedene Schichten. Unabhängig davon, wie stark sich die Datenrichtlinien auf die unteren Schichten konzentrieren, ist es auch schwierig, die Situation zu ändern, in der die mittleren und unteren Schichten ein geringes Dateneinkommen bekommen, oder noch schwieriger, ihre in der Datenschicht schon erstarrte Position zu ändern und sie in höhere Schichten zu verschieben. Durch die Teilhaberechte können nicht genutzte Datenressourcen, die privat oder öffentlich besessen sind, vollständig genutzt werden, damit mehr teilhabbare Datenprodukte, mehr Möglichkeiten und Dienste geschaffen werden, um die Datennachfrage der verschiedenen Schichten, insbesondere der Unter- und Mittelklasse, zu erfüllen. Auf diese Weise werden Ressourcen und Möglichkeiten geteilt, Barriere zwischen Datenschichten beseitigt und den unteren und mittleren Schichten Möglichkeiten gegeben, ihre Situation zu verbessern. Die Einrichtung der Teilhaberechte ermöglicht allen auf verschiedenen Datenschichten, das Recht zu genießen und Datenressourcen zu nutzen, ändert das Muster, in dem die Interessen der Datenteilhabe streng nach bestimmten Faktoren wie Kette, Fähigkeit und Ressourcen usw. verteilt werden, und erweitert die Vorteile des Teilhaberechts an alle auf verschiedenen Schichten (Zhang Guoqing 2018).

Die Teilhaberechte erhöhen die Verwaltungskapazität der Regierung. Die Regierung spielt eine entscheidende Rolle bei der Zuweisung von Datenressourcen und beeinflusst die Verteilung der Dateninteressen. In der traditionellen Ordnungsform ist es ganz schwierig, ein Gleichgewicht zwischen Effizienz und Fairness zu finden. Mit dem Teilhaberecht kann die Regierung jedoch aufgrund ihrer starken Datenkapazität institutionelle Innovationen erzielen, Regierungsfunktionen transformieren, die Verwaltungskapazität erhöhen, ein dynamisches Gleichgewicht zwischen den Funktionen der Regierung und des Marktes herstellen und ein Gleichgewicht herstellen zwischen Effizienz und Fairness, die auch der größte gemeinsame Teiler von Regierung und Markt ist. Einerseits mobilisieren die Teilhaberechte den Fluss von Personal, Kapital und Ressourcen in höchstem

Maße, beleben verschiedene Faktoren der Entwicklung der Datenindustrie, vermehren den Reichtum an öffentlichen Daten und erweitern das Wohlergehen der Daten auf mehrere Personengruppen. Indem sie das Teilhaberecht ausüben, werden Unternehmen aktiv, um Dateneffizienz zu erreichen und soziale Verantwortung zu übernehmen, das die wirtschaftlichen und sozialen Interessen maximiert, die durch Daten hervorgerufen werden. Andererseits soll sich die Regierung an die Nachfrage der Öffentlichkeit nach Daten orientieren, um qualitativ hochwertige Datenprodukte und -dienste durch Teilhaberechte anzubieten, die Begeisterung, Initiative und Kreativität aller Parteien freizusetzen, um Weisheit und Stärke von allen Seiten zu bündeln und die Interessen aller Teilnehmer zu wahren. Dies hilft, die Probleme des Eigentums an öffentlichen Datenressourcen und der Verteilung des inkrementellen Datenwerts zu lösen und das Gewinngefühl der Menschen zu stärken (Tian Xinqiao & Zhang Guoqing 2018).

Das Teilhaberecht gewährleistet Fairness und Gerechtigkeit im Bereich der Daten. Die Datenteilhabe als eine neue Art des Ressourcenzuweisungsmodells lindert das Problem der unausgewogenen Verteilung der Datenressourcen zwischen Regierung und Markt, verringert die Ungerechtigkeit der Zuweisung von Datenressourcen und der sekundären Datenzuweisung und überwindet die Ungleichheit bei Datentransaktionen und die daraus resultierende Verschwendung von Datenressourcen, die das traditionelle Modell mit sich gebracht und durch Informationsasymmetrie entstanden hat. Das Teilhaberecht gleicht die Vernachlässigung des Marktes für soziale Gerechtigkeit in Bezug auf Daten aus, ermöglicht allen Mitgliedern der Gesellschaft, alle Arten von Datenressourcen gleichermaßen zu nutzen und Datenrechte und wirtschaftliche Interessen gleichberechtigt zu erhalten und der Öffentlichkeit die Möglichkeit zu geben, grundlegenden Datenwert zu genießen. Die Datenteilhabe fungiert als Koordinator zwischen der Regierung und dem Markt und gibt den Menschen gleiche Chancen hinsichtlich des Zugangs zu, der Nutzung von und der Einnahmen aus Datenressourcen. Das Teilhaberecht bietet allen Mitgliedern der Gesellschaft einen enormen Spielraum für gleiche Rechte auf Datenressourcen und verwirklicht die Verlagerung des Schwerpunkts von der Umverteilung von individuellen Vermögen und öffentlichen Vermögen auf die gleichmäßige Teilhabe an Datenressourcen. Unter den Umständen einer wachsenden

Lücke im Datenreichtum ist es notwendig, diese mittels Teilhaberechte zu regulieren und zu verbessern. Daher müssen die Teilhaberechte sowohl zum Schutz des Eigentumsrechts auf privaten Daten als auch zur Gleichberechtigten Teilhabe an grundlegenden Datenressourcen beitragen, um Datengerechtigkeit zu erreichen (Tian Xinqiao & Zhang Guoqing 2018).

(III) Wirtschaftlicher Wert der Teilhaberechte

Die digitale Wirtschaft hat die treibende Kraft und das Modell der wirtschaftlichen Entwicklung grundlegend verändert. Der Vorschlag für Teilhaberecht motiviert die Menschen, Daten zu produzieren und zu teilen und bietet endlose Datenressourcen für Entwicklung der digitalen Wirtschaft. Der Bau einer digitalen Wirtschaft mit Daten als Schlüsselemente und eines auf Teilhabe basierenden Verteilungsmechanismus der Dateninteressen wird die tief gehende Integration der digitalen Wirtschaft und Teilhabewirtschaft unweigerlich fördern.

Das Teilhaberecht fördert Reform des Eigentumsrechtssystems. Das Eigentumsrechtssystem ist ein wichtiger Bestandteil moderner Wirtschaftssysteme. In den bestehenden Theorien über Eigentumsrecht sind Eigentumsrechte die gesetzliche Manifestationsform des Verhältnisses im wirtschaftlichen Eigentumssystem, wozu Eigentumsrecht, Besitzrecht, Dispositionsrecht, Nutzungsrecht, Ertragsrecht, Verfügungsrecht usw. gehören. Aktuelle Wirtschaftssysteme betonen die Vollständigkeit, Unveräußerlichkeit und Unverletzlichkeit von Eigentumsrechten, sodass das Eigentumsrechtssystem daher wetteifrig und exklusiv ist. Zeitgleich drängt die Exklusivität des Eigentumsrechtssystems aufgrund der großen Lücke in Bezug auf Ressourcen und Wohlstand die Ressourcen und den Wohlstand auf dem Markt kontinuierlich auf eine kleine Anzahl von Menschen, führt die Transaktion und Zirkulation von Eigentumsrechten zu einer übermäßigen Steifigkeit und behindert die wirtschaftliche Entwicklung. Daher ist die übermäßige Betonung der Vollständigkeit, Unveräußerlichkeit und Unverletzlichkeit der Eigentumsrechte ist dem freien Fluss von Talenten, Kapital und Ressourcen sowie der gesunden und freien wirtschaftlichen Entwicklung abträglich (Zhang Guoqing 2018). Das Teilhaberecht bietet

einen neuen Ansatz für Beseitigung der Nachteile des Eigentumsrechtssystems. Das Teilhaberecht bedeutet Teilhabe an Nutzungsrecht der Teilhabedaten unter dem Vorbehalt des Dateneigentums und hat so einen neuen Begriff in Bezug auf Eigentumsrecht gebildet. Diese neue Sichtweise stellt ein Modell der zweistufigen Struktur dar: Auf der oberen Ebene befindet sich das Eigentum, das entscheidet, wem die Daten gehören; auf der unteren Ebene gibt es das Teilhaberecht, das an das Nutzungsrecht und Ertragsrecht von Daten teilhat. Da Daten mit anderen geteilt werden, damit mehr Menschen sie nutzen können, ist günstig für Aktivierung der Datenressourcen. Die Grundphilosophie des Teilhaberechts ist, dass „man will Daten nicht besitzen, sondern nutzen“. Dies dient im Wesentlichen dazu, das Dateneigentumsrecht abzuschwächen und das Nutzungsrecht und Ertragsrecht auf Daten zu bekräftigen, um die Umwandlung der Sichtweise vom privaten Dateneigentumsrecht zur Teilhabe an Datenrechten zu fördern, den freien und geordneten Verkehr von Datenressourcen zu verwirklichen und die Effizienz der Zuweisung von Datenressourcen zu erhöhen. Während das Teilhaberecht die Verschwendung von Ressourcen verringert, erweitert es auch die Kanäle für bessere Nachfrage der Menschen nach Daten und vergrößert den Umfang der Datenfreiheit. Mit anderen Worten bietet das Teilhaberecht der Menschheit einen Weg dafür, dass man das bekommt, was er will und die Datenfreiheit verwirklicht wird, ohne Datenressourcen in seinen Besitz zu nehmen (Han Jing u. Pei Wen 2017).

Das Teilhaberecht erhöht den Konsumentenrestwert. Der Konsumentenrestwert bezieht sich auf die Differenz zwischen dem Spitzenpreis, den ein Konsument bereit ist, für eine bestimmte Menge einer Ware zu zahlen, und dem tatsächlichen Preis, den er dafür bezahlt. Dieser Begriff stammt aus der Alfred Marshalls Grenznutzen-Theorie und wird verwendet, um das zusätzliche Erlös der Verbraucher zu messen. Einerseits bietet das Teilhaberecht den Verbrauchern mehr Datenkanäle zur Wahl, was die Monopolstellung der Datenproduzenten schwächt, die Kräfte auf dem Datenmarkt verteilt und die Passivität der Datenkonsumenten auf dem Markt verringert. Durch das Spiel um Datenpreise ist es einfacher, die Nachfrage der Datenkonsumenten zu erfüllen. Dadurch wird der tatsächliche Preis für Datenprodukte gesenkt und der Restwert von Datenkonsumenten erhöht. Andererseits öffnet das Teilhaberecht den Markt der Nießbrauchdaten, senkt die Kosten

für Datentransaktionen, verbessert die Nutzungsrate von Datenressourcen und schafft mehr Datenreichtum. Infolgedessen füllt das Teilhaberecht die Lücke zwischen Angebot und Nachfrage von Daten und ermöglicht, die Datenressourcen in der Gesellschaft völlig genutzt zu werden. Dadurch wird erreicht, dass beide Seiten von Angebot und Nachfrage genauer, freier und geordneter aufeinander abgestimmt und die Opportunitätskosten sowie der von den Verbrauchern tatsächlich gezahlte Datenpreis gesenkt werden, wobei ein höherer Datenwert für die Teilnehmer auf Mikroebene geschaffen und somit der Restwert der Datenverbraucher erhöht werden kann (Zhang Yuming 2017, S. 429–431).

Das Teilhaberecht ändert das Wettbewerbsparadigma. Das Teilhaberecht ändert die traditionelle Wettbewerbslogik des Nullgewinnspiels und verwirklicht die Transformation hin zu einem neuen Wettbewerbsparadigma, das auf dem Teilhabewert basiert. Aus Sicht der Geschäftspraxis verlagert das Teilhaberecht den Fokus der Datenunternehmen vom wirtschaftlichen Wert der Daten auf den Teilhabewert von Daten und zwingt sie auch, ihr Anstreben nach Erlösen von wirtschaftlichen Einkommen der Daten auf universale Datenerträge zu erweitern. Daher ist es die realistischste Wahl, Wettbewerb und Zusammenarbeit auf der Grundlage des Teilhaberechts durchzuführen, um das Potenzial von Unternehmen zur Schaffung von Datenreichtum und zur Erzielung umfassender Datenerlöse voll auszuschöpfen. Man kann sagen, Datenwettbewerb und -Zusammenarbeit sind eine Einheit des Verhältnisses zwischen relevanten Unternehmen. Sie funktionieren zusammen, beeinflussen sich gegenseitig und können sich unter bestimmten Bedingungen ineinander verwandeln. Einerseits vergrößert die Ausübung des Teilhaberechts durch Unternehmen den Umfang des Datenaustauschs, beschleunigt die Verbreitung aller Arten von Daten, steigert die Nutzungseffizienz von Faktoren wie Datenressourcen, Technologien und Diensten usw. und entfaltet in größerem Maße die Vorteile von Datenressourcen und Kapital etc., regt Dateninnovationen an, erweitert die Grenzen der Möglichkeiten der Datenproduktion, damit Synergien, Kopplungseffekte und mehr Entwicklungs- und Geschäftsmöglichkeiten geschaffen werden, wobei Unternehmen auch dabei geholfen werden, Mehrwert aus der Datenteilhabe zu generieren und ihr Wertschöpfungsnetzwerk erweitert werden zu können. Auf der anderen Seite

helfen die Teilhaberechte Unternehmen dabei, die Grenzen von Daten zu durchbrechen, mehr Datenprodukte einschließlich mehr Datenressourcen, Technologien und Dienstleistungen etc. zu erhalten, die treibende Kraft und Fähigkeit für Dateninnovationen der Unternehmen zu verbessern und mehr Nutzen aus ihrem Datenrestwert zu ziehen und Datenwert für eigenen Bedarf zu schöpfen und die Nachfrage der Gesellschaft nach Daten insgesamt besser zu erfüllen (Xiao Hongjun 2015).

Das Teilhaberecht gleicht das Marktversagen aus. Das Teilhaberecht hilft dabei, die Frage der Informationsasymmetrie und die negative Äußerlichkeit des Marktes zu lösen, das Monopol zu durchbrechen und das Marktversagen auszugleichen. In Bezug auf die Beseitigung der Informationsasymmetrie fehlen Verbrauchern beim Kauf an vollständigen Daten, sie können Informationen nicht ausreichend haben, verlieren sie deswegen beim Kauf ihre vorteilhafte Position, was zu einer Situation führt, in der „schlechtes Geld gutes Geld vertreibt“. Mit den Teilhaberechten werden Informationstransparenz und Markteffizienz erheblich verbessert. In Bezug auf Verringerung der negativen Äußerlichkeit kann man durch das Teilhaberecht sein Ziel erreichen, Daten zu nutzen und daraus zu verdienen, ohne sein privates Dateneigentum zu vermehren. Das reduziert den Besitz von Datenproduktionsmitteln, vermeidet in maximalem Maße den Einfluss negativer Äußerlichkeit und mindert den Druck der Datenknappheit. Deshalb kann das Teilhaberecht die Frage der Informationsasymmetrie negativer Äußerlichkeit auf dem Markt lösen, die genaue Anpassung und volle Ausnutzung von Datenressourcen zu fördern und das Marktversagen ausgleichen (Zhang Yuming: 2017, S. 445–447).

Literaturverzeichnis

- Cheng Tongshun u. Shi Meng: „Recht auf öffentliche Daten und politische Demokratie“, in Jianghai Academic Journal, 4/2018.
- Dong Yurong: „Das Konzept der Gerechtigkeit und das Interessengleichgewicht der Teilhabe: Weg zur Verwirklichung der Integration von privaten Rechten und sozialer Nützlichkeit“, in Sozialwissenschaften in Guangxi, 10/2010.

- Du Zhenhua u. Cha Hongwang: „Analyse der Realität des Dateneigentumsrechtssystems“, in *Chongqing Sozialwissenschaft*, 8/2016.
- Guan Dehua u. Kong Xiaohong: „Die Evolution der westlichen Werttheorie“, China Economic Publishing House, 2013.
- Han Jing u. Pei Wen: „Idee der Teilhabe, Entwicklung der Teilhabe-Wirtschaft und innovative Reform der Wirtschaftsstruktur“, in *Journal Wirtschaftsforschung Shanghai*, 8/2017.
- He Zhe: „Form der menschlichen Gesellschaft und Ordnungsbau im Zeitalter der Cyberzivilisation“, in *Sozialwissenschaft Nanjing*, 4/2017.
- Hu Shouyong: „Globale historische Bedeutung der Philosophie der Teilhabe der Entwicklung“, *Studien zum Marxismus*, 4/2018.
- Li Jianhui & Gong Xiaole: „Über persönliche Interessen hinaus: Altruistisches Problem von Darwin und seine Lösung“, in „Forschung über Dialektik der Natur“, 9/2009.
- Li Jianhui u. Xiang Xiaole: „Hinweg über das Eigeninteresse: Darwins Altruismus-Puzzle und seine Lösung“, in *Studien zur Dialektik der Natur*, 9/2009.
- Liu Genrong: „Teilhabe-Wirtschaft: Ein Umstürzler des traditionellen Wirtschaftsmodells“, *The Economists*, 5/2017.
- Liu Heling: „Von der Wettbewerbsentwicklung zur kooperativen Entwicklung: Neue Entwicklung von Darwins Theorie der natürlichen Selektion“, in „Wissenschaft, Technologie und Dialektik“, 1/2005.
- Liu Ling: „Historische Ursprünge und ein einheitliches Governance-Muster für Fairness und Gerechtigkeit sowie gemeinsame Entwicklung“, *Humanities & Social Sciences Journal der Hainan University*, 4/2019.
- Long Rongyuan u. Yang Guanhua: „Studie über Datenrechte, Datenrechtssystem und Datenrechtsgesetz“, *Journal of Law and Technology*, 5/2018.
- Lu Xiaohua: „Informationseigentumsrecht: Ein neues Modell zum Schutz des Vermögens aus zivilrechtlicher Sicht“, *Rechtsverlag*, 2009.
- Luo Ying: „Die Position der Teilhaberechte unter den Umständen einer umfassenden Vertiefung der Reform“, in „Sucher“, 6/2014.
- Meng Kui: „Vergleich von drei wichtigen Werttheorien in der Ökonomie“, in *Wirtschaftsbericht*, 7/2013.
- Miao Ruidan u. Dai Junyuan: „Forschung zum theoretischen Konnotations- und Praxispfad der gemeinsamen Entwicklung“, in *Studie der ideologischen Bildung*, 3/2017.
- Peter H. Diamandis & Steven Kotler: „Reichlich: 4 große Kräfte, die die Zukunft der Menschheit ändern“, übersetzt von Jia Yongmin, *Volksverlag Zhejiang*, 2014.
- Schlüssel-Labor von Big Data-Strategie: „Blockdaten 5.0: Theorie und Methode der Datensozialwissenschaft“, *CITIC Verlag*, 2019.

- Schlüssel-Labor der Big Data Strategie: „Datenrechtsgesetz 1.0: theoretische Grundlage des Datenrechts“, Verlag der sozialwissenschaftlichen Literatur, 2018.
- Tian Xinqiao u. Zhang Guoqing: „Der Weg zu Teilhabe – Warum der Sozialismus richtig ist“, in *Zhejiang Sozialwissenschaft*, 2/2018.
- Wang Liming: „Datenteilhabe und Schutz personenbezogener Daten“, in *Moderne Rechtswissenschaft*, 1/2019.
- Wang Liming: „Forschungen zum Persönlichkeitsrecht“, Verlag der chinesischen Remin Universität, 2005.
- Wang Yan u. Ye Ming: „Konflikt und Gleichgewicht zwischen der Teilhabe an persönlichen Daten und dem Schutz der Privatsphäre im Zeitalter der künstlichen Intelligenz“, in *Zeitschrift der theoretischen Anleitung*, 1/2019.
- Xiao Hongjun: „Wert der Teilhabe, Geschäftsökosystem und Transformation des Wettbewerbsparadigmas von Unternehmen“, in *Reform*, 7/2015.
- Zentrales Büro für Zusammenstellung und Übersetzung Sämtliche Werke von Marx und Engels (Bd. 23). Volksverlag, 1972.
- Zhang Guoqing: „Gerechtigkeit als Teilhabe: Über das Ungleichgewicht in der sozialen Entwicklung Chinas“, in *Zhejiang Academic Journal*, 1/2018.
- Zhang Xinbao: „Gesetzlicher Schutz des Rechts auf Privatsphäre“, *Volksmassen Verlag*, 1998.
- Zhang Yujie: „Über Rechtsordnung für Rechte und Risiken von Robotern im Zeitalter der künstlichen Intelligenz“, in *Orientalisches Recht*, 6/2017.
- Zhang Yuming: „Teilhabeökonomie“, *Wissenschaftspresse*, 2017.
- Zhao Hong: „Sozialstaat und soziale Grundrechte der Bürger: Erweiterung und Einschränkung der Grundrechte im Sozialstaat“, in *Zeitschrift für Forschung über Gesetzvergleich*, 5/2010.
- Zheng Jianjun u. Fu Xiaojie: „Der Einfluss altruistischer Motivation auf Wissensaustausch zwischen Grund- und Sekundarschullehrern: Die moderierenden Rollen der organisatorischen Identifikation und der wahrgenommenen organisatorischen Unterstützung“, in *Psychologische Entwicklung und Bildung*, 4/2019.
- Zhou Shuyun u. Luo Xueying: „Analyse des Inhalts des Rechts auf Zugang zu Informationen“, in *Informationsstudien: Theorie und Praxis der Informationsnachrichten*, 5/2014.
- Zhou Shuyun u. Wang Haoyun: „Analyse von Objekten des Rechts auf Zugang zu Informationen“, in *„Bibliothek“*, 1/2015.
- Zhou Shuyun: „Analyse zu Subjekt des Rechts auf Zugang zu Informationen“, in *„Bibliothek“*, 5/2014.

Datensouveränität

Datensouveränität ist ein wichtiger Bestandteil der staatlichen Souveränität und eine Manifestation und natürliche Erweiterung der staatlichen Souveränität im Datenraum. Datenhoheit bezieht sich auf die Befugnis des Staates, Daten in seinem Herrschaftsbereich zu generieren, verbreiten, verwalten, kontrollieren, nutzen und zu schützen. Es ist eine unvermeidliche Anforderung für alle Länder, die Souveränität und Unabhängigkeit des Staates zu wahren und das Datenmonopol und den Hegemonismus im Zeitalter von Big Data zu bekämpfen. Die Datenhoheit umfasst folgende Rechte: das Recht auf Datengerichtbarkeit, Recht auf Datenunabhängigkeit, Recht auf Datengleichheit und Recht auf Datenselbstverteidigung. In der Praxis hat der Wettbewerb zwischen verschiedenen Ländern um Datenhoheit zu einem Zustand der Unordnung geführt, der Konflikte zwischen mehreren Gerichtsbarenkeiten und Dilemma der staatlichen Sicherheit aufweist. Gleichzeitig ist die Datenhoheit ein Bereich mit vielen sich überschneidenden Interessen, der mit Problemen wie Datenhegemonismus, Datenprotektionismus, Datenkapitalismus, Datenterrorismus usw. konfrontiert. Um die Datensicherheit und Datenhoheit zu gewährleisten, soll die internationale Gemeinschaft hart und aktiv daran arbeiten, ein Verwaltungssystem für Datenhoheit aufzubauen, die Zusammenarbeit im Zusammenhang mit dem System der Datenhoheit zu fördern und ein Rechtssystem für Datenhoheit, das den heutigen Entwicklungsbedürfnissen der Welt entspricht und sie erfüllt, aufzubauen, um auf diese Weise den globalen Datenfluss auf der Bahn eines soliden internationalen Rechtssystems zu stellen, so dass die ganze Menschheit davon profitieren kann.

Abschnitt I Aufstieg der Datensouveränität

Der grenzüberschreitende Datenfluss hat erhebliche Auswirkungen auf die traditionelle Wahrnehmung der staatlichen Souveränität und führt zur Abschwächung der staatlichen Souveränität und zur Entstehung der Datenhoheit im richtigen Moment. Die Datensouveränität hat die Cyber-Souveränität geerbt und entwickelt diese weiter. Auf der nationalen Ebene haben die Konzepte der Datensouveränität und der Cybersouveränität denselben Ursprung, d.h. beide haben sich aus dem Begriff der staatlichen Souveränität entwickelt und sind wichtige Bestandteile der staatlichen Souveränität. Als Produkt der staatlichen Souveränität in der Ära von Big Data entsteht die Datensouveränität, wenn der Datenraum existiert. Sie ist eine Manifestation, Erweiterung und Reflexion der staatlichen Souveränität im Datenraum. Aufgrund der Besonderheiten des Datenraums weist die Datenhoheit wichtige Merkmale wie Zeitgenossenschaft, Relativität, Kooperativität und Gleichheit usw. auf. Die Vorlage der Datensouveränität ist für den Schutz der Datensicherheit und den Aufbau einer Cybermacht von großer Bedeutung.

(I) Ursprung der Souveränität

In der frühen Entwicklungsphase der menschlichen Zivilisation gab es noch keine Staatsform und die Menschen hatten auch keine Ahnung von Souveränität. Mit dem Aufkommen des Krieges und der Gründung von Staaten nahmen die Idee und das Konzept der Souveränität allmählich Gestalt an und wurden immer klarer. Wissenschaftler verschiedener Zeiten und aus verschiedenen Ländern haben die Souveränität aus verschiedenen Perspektiven herausgearbeitet. Jetzt ist es sinnvoll, die frühere Literatur zur Souveränität zu überprüfen und die Merkmale der Souveränität in verschiedenen Zeiträumen zu klären, da dies uns helfen kann, der staatlichen Souveränität im Zeitalter von Big Data eine neue Konnotation hinzuzufügen.

I. Keimung der Idee der Souveränität

Die Auffassung der „Souveränität“¹ kann bis in die Antike zurückreichen und keimte in einer bestimmten Zeit und in einem bestimmten Raum. Sie ist das Ergebnis sozialer Veränderungen und wirtschaftlicher Entwicklung. Die Existenz der Souveränität ist eine Voraussetzung für menschliche Handlungen und kann die Gesellschaft von Unordnung zu Ordnung führen. Während der Zeit des alten Griechenlands und des antiken Roms waren die Staaten getrennt und es gab viele Probleme in und aus ihnen heraus. So erkannten die alten Philosophen, dass der einzige Weg, inneren Streit zu verhindern und der Invasion von Feinden zu widerstehen, darin bestand, einen einheitlichen und zentralisierten Staat zu schaffen. Deshalb haben sie den langen und anstrengenden Weg zur Untersuchung des Klerikalismus und der Herrschergewalt eingeschlagen. Wie man sieht, haben die frühen Philosophen die Existenz von Souveränität schon lange bemerkt und die Konnotationen des Konzepts der Souveränität entsprechend studiert. Obwohl sie das politische Konzept der „Souveränität“ nicht explizit vorgebracht haben, kamen ihre Forschungen über die Herkunft von Staaten, die Arten der Staatsformen und die Regierungsführung von Staaten unserem heutigen Konzept von „Souveränität“ im Wesentlichen sehr nahe, und ihre Bemühungen hatten den Grundstein für die Erstellung des Konzepts der „Souveränität“ in der Aufklärungszeit gelegt.

Es wurde angenommen, dass Aristoteles der Erste ist, der die Idee der Souveränität zuerst erklärt hat. In seinem Buch „Politik“ wies er darauf hin, dass „die Staatsform die Grundlage aller politischen Organisationen

1 Einige Wissenschaftler glauben, dass Souveränität und Staatssouveränität zwei unterschiedliche Begriffe sind: „Staatssouveränität ist nur eine der Manifestationsformen souveräner Subjektivität ... Wenn wir Souveränität nicht von staatlicher Souveränität unterscheiden, wird es für uns schwierig sein, die Konnotation staatlicher Souveränität genau zu verstehen.“ Aber im Allgemeinen macht man nicht zu viel Unterschied zwischen Souveränität und staatlicher Souveränität und betrachtet sie als unterschiedliche Ausdrücke desselben Begriffes. Gleichzeitig unterscheidet das Buch nicht die Begriffe zwischen Souveränität und staatlicher Souveränität, da der Begriff der Souveränität für den Staat in Bezug auf seine moderne Bedeutung unweigerlich relevant ist.

in einem Stadtstaat ist, insbesondere die Organisationen der ‚höchsten Herrschaftsmacht‘, die von der Politik bestimmt“ (Aristoteles 1996, S. 129). Nach seiner Ansicht ist die Anzahl der Herrscher das Hauptkriterium für die Klassifizierung des Regierungssystems, während der Staat die Regierungsform mit der größten Anzahl von Herrschern und anderen Regierungsformen überlegen ist. Daher hat der Staat die Macht zu herrschen. Er bestand auf die Rechtsstaatlichkeit statt auf Menschenherrschaft und glaubte, dass das Gesetz der beste Herrscher ist und dass die Formulierung von Gesetzen die Meinungen der Mehrheit widerspiegeln und so hat es einen größeren Konsens und Wünschbarkeit. Daraus ist ersichtlich, dass die Idee, dass der Staat die höchste Macht hat, erst jetzt ihre anfängliche Form hat. Trotz der Tatsache, dass Aristoteles den Begriff „Souveränität“ nicht ausdrücklich verwendete, hatte aber bereits erklärt, dass die staatliche Souveränität die höchste Autorität in inneren Angelegenheiten hat.

Die früheste Form staatlicher Souveränität entstand aus den Gedanken der alten römischen Juristen, dass das Volk der autoritäre, einzige und der ultimative Träger im Staat ist und aus dem tiefen Verständnis dafür, dass das Volk das Subjekt, der Besitzer und Durchführer der staatlichen Souveränität ist. Die Idee der Souveränität im alten Rom kann sich in einem berühmten Sprichwort widerspiegeln: „Da nun das Volk alle seine Rechte und Macht dem König überlassen hat, so soll der Wille des Königs die Rechtskraft haben“ (Chen Xujing 2010, S. 10). Dieses Sprichwort wurde zu verschiedenen Zeiten unterschiedlich interpretiert. Wenn der Kaiser oder König die höchste und uneingeschränkte „absolute Macht“ genießt, gelten sie als Souveränitätsbesitzer, aber diese Souveränität wurde ihnen tatsächlich durch eine natürliche Übertragung der Rechte vom Volk verliehen. Die Macht des Kaisers oder Königs befindet sich in einem dynamischen Prozess des Aufstiegs oder Niedergangs. Seine Macht wird vom Volk anvertraut. Das Anvertrauen bedeutet jedoch nicht aufzugeben, und das Volk besitzt immer noch die höchsten Kernrechte. Obwohl sich diese Souveränitätsgedanken stark von den modernen Souveränitätsgedanken unterscheiden, kann man aber daraus ersehen, dass der Kerninhalt in dem Glauben liegt, dass die „Souveränität dem Volk gehört“.

2. Entwicklung der Souveränitätstheorie

Der französische Philosoph Jean Bodin war der erste in der Geschichte, der der Souveränität eine systematische und spezifische Definition gab. Ihm zufolge ist Souveränität die einheitliche, untrennbare und höchste Macht über alle Gesetze, die ein Staat genießt (Zhu Qi 2015). In seinen Sechs Büchern des Commonwealth (Sechs Livres de la République) weist Bodin darauf hin, dass eine Reihe von Familien und der von ihnen besitzenden gemeinsamen Vermögen einen Staat bildet, der die höchste Souveränität hat. Eine solche souveräne Macht unterliegt keinem Gesetz. Sie ist die ewige, absolute und höchste Macht eines Staats. Bodin erläuterte systematisch den Begriff und das Attribut der Souveränität. Obwohl er die Legitimität der Souveränität nicht stichhaltig erklärte, passte seine Idee zu den sozialen Situationen in Frankreich und der Welt seiner Zeit und legte eine solide Grundlage für die Weiterentwicklung der Souveränitätstheorie. Bodins Gedanken zur Souveränität wurden als Ursprung der modernen Theorien des souveränen Staates angesehen und spielten zugleich auch eine positive Rolle bei der Umsetzung der modernen Gedanken der Souveränität.

Thomas Hobbes erbt Bodins Gedanken der Souveränitätstheorie und auf dieser Basis erweiterte und bereicherte sie. Er befürwortete „natürliche Menschenrechte“ (jus natural) und glaubte, dass alle Menschen frei und gleich geschaffen sind und dass jeder die gleichen natürlichen Rechte auf natürlichen Ressourcen hat (Yang Xiaotong 2018). Die Ressourcen sind jedoch begrenzt. Daher treten Menschen einem Gesellschaftsvertrag bei und geben ihre Macht auf, wodurch sie an den Gesellschaftsvertrag gebunden sind, ohne Erlaubnis ihres „Souveräns“ darf Niemand seine Persönlichkeit von einem Anerkannten dem anderen oder einer Versammlung von Menschen abzutreten, weil diese Persönlichkeit im gegenseitigen Einvernehmen zwischen Menschen gebildet worden ist und diese „Ermächtigungshandlung“ schon bei der Vertragsunterzeichnung legalisiert worden ist. Hobbes glaubte, dass der „Souverän“ uneingeschränkt und oberstes Gebot sei und dass das Volk nur das Recht habe, zu entscheiden, ob es einen Gesellschaftsvertrag abschließt oder nicht: Die Entscheidung, einen solchen Vertrag zu

unterzeichnen, erklärt die Beendigung seiner politischen Rechte. Man kann sagen, dass Hobbes „Theorie der Souveränität“, die gerechtfertigt erscheint, tatsächlich aber widersprüchlich ist. Trotzdem soll sein Wert bei der Förderung der Entwicklung der Souveränitätstheorie subjektiv anerkannt werden.

Jean-Jacques Rousseaus Gedanke an die Volkssouveränität ist ein großer Sprung in der Entwicklung der Souveränitätstheorie. Es stürzte die feudale autokratische Monarchie radikal und führte das Volk in eine neue Gesellschaft der Freiheit und Gleichheit. Rousseau vertrat die Auffassung, dass die Souveränität nicht übertragbar ist, dass die Volkssouveränität die Verkörperung des „allgemeinen Willens“ ist, dass sie die Schnittstelle des Willens aller bei der Unterzeichnung eines Gesellschaftsvertrags darstellt und dass die Macht übertragbar aber das Bewusstsein jedoch nicht übertragbar ist. Basierend auf der Idee, dass die Souveränität nicht übertragbar ist, ist sie auch unteilbar, weil das Bewusstsein universell ist und, sobald es geteilt ist, bedeutet, dass es nicht existiert. Wenn das Bewusstsein als Wille des Volkes als Entität betrachtet wird, bedeutet dies, dass der allgemein anerkannte und offene Wille eine souveräne Vereinbarung ist und Gesetze darstellt (Jean-Jacques Rousseaus 2006, S. 20–21). In Rousseaus Souveränitätstheorie ist die Souveränität relativ absolut: Sie ist im Rahmen einer universellen Vereinbarung absolut, aber nicht außerhalb des Rahmens. Rousseau stellte die Theorie der Volkssouveränität auf der Grundlage des Niveaus auf, das die Souveränitätsgedanken seiner Vorgänger erreicht hatten. Sie war eine Zusammenfassung aller früheren Vorschläge und ein Sprung nach vorne; darüber hinaus kündigte sie die Weiterentwicklung der Souveränitätstheorie an, anstatt sie abzuschließen (siehe Tabelle 4-1).

Tabelle 4-1 Einige Souveränitätstheorien

Zeit	Figur	Souveränitätstheorie
1530– 1596	Jean Bodin	Die erste systematische und spezifische Definition der Souveränität: Die Souveränität ist ein wichtiges Symbol des Staates und die höchste Macht gegenüber Bürgern und Untertanen, die frei von gesetzlichen Beschränkungen sind. Souveränität ist die oberste Autorität im Inland und das Recht auf Unabhängigkeit und Gleichheit gegenüber der Außenwelt.
1583– 1645	Hugo Grotius	Die Prämisse des Völkerrechts ist die staatliche Souveränität. Staatssouveränität bezieht sich auf die höchste Regierungsmacht eines Staates, d.h. die Macht, die es dem Souverän ermöglicht, zu handeln, ohne vom Willen anderer oder vom Gesetz beherrscht zu werden. Grotius ist gegen die Volkssouveränität und befürwortet die Souveränität des Monarchen. Die Souveränität dient als Grundlage für die Existenz eines Staates und als Voraussetzung dafür, dass ein Staat Gegenstand des Völkerrechts ist.
1588– 1679	Thomas Hobbes	Einzelpersonen übertragen natürliche Rechte auf einen „Souverän“. Diese Theorie kritisiert das göttliche Recht der Könige, setzt sich für die Staatsmacht ein und verleiht der „Souveränität“ einen höchsten Status.
1632– 1704	John Locke	Die staatliche Souveränität hängt mit der politischen Macht und der höchsten Macht zusammen und umfasst die gesetzgebende Gewalt, die Exekutivgewalt und die föderative Macht. Es gibt zwei Ansätze für die staatliche Souveränität: die parlamentarische Souveränität und die Volkssouveränität. Souveränität ist nicht gleichbedeutend mit absoluter Souveränität.
1712– 1778	Jean-Jacques Rousseau	Die früheste vollständige Theorie der Volkssouveränität: Die staatliche Souveränität ist unteilbar und nicht übertragbar. Jeder Ausdruck und jede Anwendung der Menschenrechte muss den Willen des Volkes widerspiegeln; das Gesetz ist der „allgemeine Wille“, was bedeutet, dass alle vor dem Gesetz gleich sind und der Monarch auch nicht über dem Gesetz stehen kann.

3. Aufstellung der modernen Souveränität

Die Souveränität ist niemals ein statisches Konzept. Es ändert sich ständig mit der gesellschaftlichen Praxis, den wissenschaftlich-technologischen Innovationen und der wirtschaftlichen Entwicklung und wandelt sich elastisch. Es gibt zwei Gründe für die Entstehung des modernen Konzepts der Souveränität: Der eine ist die interne Motivation, die erzeugt wird, wenn ein souveräner Staat Überleben, Interessen und Entwicklung verfolgt; und der andere ist die externe höhere Gewalt, der ein souveräner Staat in einem sich verändernden internationalen Umfeld ausgesetzt ist. Die moderne Souveränität ist ein Erfolg als Meilenstein in der Entwicklung der menschlichen Zivilisation, da sie die Art und Weise, wie souveräne Staaten miteinander kommunizieren, verändert und die große Reform der internationalen Systeme und des Völkerrechts vorantreibt. Einerseits kann die Souveränität von Vorschriften und Regulierungen durch nationale Gesetze nicht getrennt werden; und andererseits wird sich die Theorie der Souveränität mit der Zeit sicherlich weiterentwickeln und bereichern. Daher ist die Entstehung der modernen Souveränitätstheorie nicht nur ein unvermeidliches Ergebnis unserer Bemühungen, Chaos und Unordnung einzudämmen und eine solide Rechtsordnung zu schaffen, sondern auch ein Grundbedürfnis für den Übergang der menschlichen Gesellschaft von der industriellen zur digitalen Zivilisation.

Die moderne Souveränität ist eine Fortsetzung und Entwicklung der traditionellen Souveränität. Mit fortschreitender Globalisierung ist die traditionelle Souveränität mit vielen Herausforderungen konfrontiert, wie dem Aufbau und der Entwicklung internationaler Organisationen, der häufigeren transnationalen Zusammenarbeit und der Entstehung einer Vielzahl internationaler Institutionen und Mechanismen. Diese Herausforderungen durchbrechen die territorialen Grenzen der traditionellen Souveränität und verwischen die Grenzen der Souveränität. Auf der Grundlage des Konzepts der traditionellen Souveränität entstand die moderne Souveränitätstheorie, die Elemente wie Kommunikation und Zusammenarbeit, wirtschaftlichen Austausch und Teilhabe an Ressourcen mit internationalen Organisationen umfasst. Die moderne Souveränität bedeutet nicht mehr die absolute Unabhängigkeit in militärischer, politischer, wirtschaftlicher und technologischer Hinsicht, sondern die relative Unabhängigkeit,

um sich an den Trend der Globalisierung anzupassen. Auf der Basis der traditionellen Souveränität hat die moderne Souveränitätstheorie einen breiteren Anwendungsbereich und einen umfassenderen Inhalt als Reaktion auf die Entwicklung neuer territorialen Gebiete. „Die traditionelle Souveränität ist nicht nur widersprüchlich gegen die Praxis, sondern hat die Gedankenweise der Menschen beschränkt und Hände und Füße des Staates auch gebunden“ (Liu, Qingjian 2004). Alles in allem ist die moderne Souveränität eine Kombination aus Theorie und Praxis, durchbricht die Grenzen der traditionellen Souveränität und löst die Zwangslage, mit der wir derzeit in Bezug auf die Souveränität konfrontiert sind.

Die moderne Souveränität ist eine neue Form der staatlichen Souveränität. Es werden keine neuesten Rechte geschaffen. Da die Verlagerung des Makro-Sichtfeldes der Menschheit von der physischen Welt in den virtuellen Raum Chance dafür bietet, Regel und Vorschriften zu erstrecken und zu vervollständigen, so ist die Entstehung der „fünften Domäne“ das Ergebnis der kontinuierlichen Weiterentwicklung der Souveränitätstheorie in der Praxis. Obwohl es schwierig ist, eine greifbare Grenze in diesem neuen Gebiet zu ziehen, kann die virtuelle Barriere, die mit Technologien, Kenntnissen und Kultur etc. geschaffen wurde, aber auch nicht überschritten werden. Die „fünfte Domäne“, die die Informationen und Daten der physischen Welt enthält, ist ein Teil der „global öffentlichen Domäne“ und auch ein neues Feld, um das sich die großen Länder sicherlich bemühen. Die Entstehung der „Souveränität über die fünfte Domäne“ wird die Konfrontationen zwischen verschiedenen Ländern in der „fünften Domäne“ abmildern, den internationalen Dialogmechanismus in Bezug auf die „fünfte Domäne“ verbessern und die gemeinsamen Interessen in der „fünften Domäne“ wahren. Die „Souveränität über die fünfte Domäne“ ist eine Manifestation der modernen Souveränität und eine reine Veräußerung im Bereich der Rechtstheorie im Prozess des Hinausgehens des modernen Konzepts der Souveränität über das traditionelle Konzept der Souveränität.

(II) Von der Cyber-Souveränität zur Datensouveränität

Gegenwärtig sind die traditionelle und nicht traditionelle Sicherheit miteinander verflochten. Die Bedrohungen für nicht traditionelle Sicherheit

treten zunehmend in den Vordergrund und bestürmen die staatliche Sicherheit sehr. In diesem Zusammenhang ist die Datensouveränität zu einem unweigerlichen Weg zur Wahrung der Staatssicherheit geworden. Die Datensouveränität ist Fortsetzung und Entwicklung der Cyber-Souveränität, und beide überschneiden sich in gewissem Maße. Die Entstehung der Datenhoheit zielt darauf ab, Sicherheitsprobleme zu lösen, die durch massive Daten verursacht werden. Sie unterscheidet sich in irgendeiner Weise von den mit der Cyber-Souveränität im Zusammenhang stehenden Konzepten.

1 Staatssicherheit

Die Staatssicherheit ist der Eckpfeiler der Stabilität, des Überlebens und der Entwicklung eines Landes. Basierend auf dem allgemeinen Verständnis von Sicherheit ist die Staatssicherheit in erster Linie eine Art Sicherheitszustand und beinhaltet auch die Methoden und Fähigkeiten, um einen solchen Zustand aufrechtzuerhalten und zu erreichen. Wenn der Staat in einem sicheren Zustand ist, bedeutet, dass sich der Staat in Stabilität und Ordnung befindet und das Volk kann ohne Sorgen das verfolgen, was es will und das verwirklichen, was es glaubt. Ohne staatliche Sicherheit würde es keine Stabilität und Ordnung geben, und dann müssten die Menschen alles daran setzen, um sicher zu überleben, und davon kann überhaupt keine Rede sein, den Wert des Lebens zu verwirklichen. Die Wahrung der Staatssicherheit bedeutet daher, die Grundinteressen des Landes und seiner Bevölkerung zu wahren. Die staatliche Sicherheit ist nicht nur Anliegen eines Landes, sondern auch ein Problem, mit dem die gesamte Menschheit gemeinsam konfrontiert. Die Staatssicherheit bietet wichtige Unterstützung für den Aufbau einer Schicksalsgemeinschaft der Menschheit.

Die Staatssouveränität und Staatssicherheit sind miteinander verflochten und voneinander abhängig. Die Wahrung der Staatssicherheit bedeutet also, die Gleichheit, Unabhängigkeit, Integrität und Unentziehbarkeit der Staatssouveränität zu verteidigen. Die Komplexität, Unsicherheit und Unvorhersehbarkeit der internationalen Beziehungen verbinden die staatliche Souveränität und die staatliche Sicherheit eng miteinander, und Vorschriften über die staatliche Souveränität sollen auf der Anpassung an die

internationalen Beziehungen beruhen. In der Praxis der internationalen Beziehungen gibt es überregionale und interkulturelle Interaktionen zwischen verschiedenen Ländern, und es treten verschiedene Arten von Interaktionen zwischen Ländern mit gleichen sozialen Bedingungen auf. Es ist die externe Struktur des internationalen Systems und die von verschiedenen Ländern im Interaktionsprozess erzielten Konsensvereinbarungen und der Interaktionsprozess an sich, die die Interaktionsbeziehungen zwischen den Ländern aufrechterhalten und die Form der Interaktion zwischen den Ländern bestimmen. Die Struktur des internationalen Systems hat großen Einfluss auf die staatliche Souveränität, spornt das Bewusstsein aller Länder an, ihr Bestes zu geben, um ihre staatliche Souveränität zu schützen, und drängt immer mehr Länder, der staatlichen Souveränität und der staatlichen Sicherheit bei der Formulierung von Strategien im Zusammenhang mit auswärtigen Angelegenheiten sehr hohe Priorität einzuräumen.

Gegenwärtig steht die Staatssicherheit nicht nur vor Herausforderungen in traditionellen Dimensionen wie Politik, Militär, Staatsgebiet und Wirtschaft usw., sondern auch einer Reihe Fragen in nicht-traditionellen Dimensionen wie Cybersicherheit und Datensicherheit gegenüber. In solch einer komplizierten Sicherheitssituation ist die Aufrechterhaltung der staatlichen Sicherheit und der Wahrung der staatlichen Souveränität zu einem realistischen Problem geworden. Die Innovationen im Bewusstsein der Souveränität und der Ausweitung des Bereichs der Souveränität sind zu einem unvermeidlichen Trend bei unseren Bemühungen für Wahrung der staatlichen Sicherheit im Zeitalter von Big Data geworden. Die Entstehung neuer Formen der Souveränität wie Cyber-Souveränität und Daten-Souveränität erbt rationell das traditionelle Konzept der Souveränität, ist aber gleichzeitig auch hochinnovativ. Sie erweitert und bereichert die Konnotation und Epitaxie der staatlichen Souveränität und hat eine wichtige leitende Bedeutung für den angemessenen Umgang mit und Behandlung von Fragen der staatlichen Sicherheit im Zeitalter von Big Data.

2. Cyber-Souveränität

Der Cyberspace ist keineswegs Ort außerhalb des Gesetzes. Die Cyber-Souveränität ist die natürliche Erweiterung der staatlichen Souveränität

im Cyberspace. Tatsächlich wird das Konzept der Cyber-Souveränität weitgehend für innere Angelegenheiten ausgerichtet, und das zentrale Anliegen ist die Aufrechterhaltung einer friedlichen und ausgeglichenen Entwicklung des Cyberspace. „Der Cyberspace wird von Menschen geschaffen, und seine intrinsischen Eigenschaften bestimmen, dass er unweigerlich auf viele rechtliche Probleme stoßen wird. Um diese Probleme zu lösen, ist ein Eingreifen auf nationaler Ebene erforderlich. Um eine nachhaltige und gesunde Entwicklung des Cyberraums aufrechtzuerhalten, müssen Regeln und Anpassungen auf nationaler Ebene erfolgen. Die zwangsläufige Folge ist die Ausweitung der staatlichen Souveränität auf den Cyberspace und die Geburt des Konzepts der Cyber-Souveränität“ (Du Zhizhao & Nan Yuxia 2014). Die Entstehung der Cyber-Souveränität bezieht einerseits den vom Internet geschaffenen virtuellen Raum in den allgemeinen Rechtsrahmen ein, damit die Behörden eine solide Rechtsgrundlage für Aufrechterhaltung der Ordnung im Cyberspace und für gesetzmäßige Netzwerksregulierung finden können, um die Interessen der Internetnutzer zu schützen. Andererseits bietet es auch eine rechtliche Garantie für die freie Meinungsäußerung und die freie Teilnahme am Cyberspace.

Die Cyber-Souveränität ist ein wichtiger und untrennbarer Bestandteil der staatlichen Souveränität. Um ein harmonisches Cyberspace-Managementsystem aufzubauen, muss man die höchste Macht der souveränen Staaten im inländischen Cyber-Management sowie die Rechte auf Gleichheit, Unabhängigkeit, Selbstverteidigung und deren Zuständigkeit bei der Teilnahme an der internationalen Cyberspace-Verwaltung respektieren. Das Recht auf Gleichstellung bedeutet, dass alle Länder gleichberechtigt an der internationalen Cyberspace-Verwaltung teilnehmen können, und es darf keine Ungleichheit in der Cyber-Souveränität geben, die auf der Größe der Länder oder der unterschiedlichen Ausstattung mit Cyber-Ressourcen beruht. Das Recht auf Unabhängigkeit bedeutet, dass Kommunikationseinrichtungen und Netzwerkgeräte in einem Land nicht ohne Erlaubnis gestört werden dürfen. Das Recht auf Selbstverteidigung bedeutet, dass souveräne Staaten alle inländischen Ressourcen mobilisieren können, um den normalen Betrieb ihrer Netzwerkinfrastruktur sicherzustellen. Unter Zuständigkeitsrecht wird verstanden, dass die physischen

Plattformen, aus denen der Cyberspace besteht, die von ihnen getragenen Daten und die damit verbundenen Aktivitäten der gerichtlichen und administrativen Gerichtsbarkeit von souveränen Staaten unterliegen (Fang Binxing, Zou Peng & Zhu Shibing 2016).

Der Vorschlag für Cyber-Souveränität ist zu einem Konsens der internationalen Gemeinschaft geworden. Aber die Liberalisierung und Grenzlosigkeit im Internet unterscheidet sich stark von der physischen Welt, in der Länder unabhängig sind und feste Grenzen haben. Die Cybersicherheit ist zu einem neuen Element der Staatssicherheit geworden. Der harte Wettbewerb zwischen dem neuen cyberspaceorientierten Ansatz und dem traditionellen Sicherheitsansatz zeigt einerseits, dass Länder auf der ganzen Welt der Teilnahme an der Cyberspace-Verwaltung Bedeutung beimessen. Auf der anderen Seite erwies sich der Aufbau eines soliden, wissenschaftlichen, effektiven und nachhaltigen internationalen Cybersicherheitssystems als gemeinsames Ziel der internationalen Gemeinschaft und der Regierungen aller Länder (Yu Zhigang 2016). Das Konzept der Cyber-Souveränität entsteht genau im Einklang mit der Entwicklungstendenz des Internets. Kein Land befindet sich wirklich außerhalb des Cyberspace, alle Länder der Welt sollen den Cyberspace als eine große Plattform gut nutzen, um die Kommunikation und den Austausch zu stärken, den Abstand des Dialogs zu verkürzen und internationale Streitigkeiten zu beseitigen. Nur mit gegenseitigem Respekt des Obersatzes für Gleichheit der Cyber-Souveränität können wir wirklich gegenseitiges Vertrauen und internationalen Konsens erreichen und ein globales Dorf für die Menschheit mit gegenseitiger Abhängigkeit wie „Du hast mich und ich habe dich“ schaffen.

3. Datensouveränität

Die Datensouveränität ist der Kerninhalt der Cyber-Souveränität. Sowohl die Cyber-Souveränität als auch die Datensouveränität sind Erweiterungen der staatlichen Souveränität in der „fünften Domäne“, die dem traditionellen Konzept der staatlichen Souveränität und verwandten Theorien neue Elemente hinzufügen und sie an die neuen Situationen in einer neuen Ära anpassen. Sie bedeuten nicht nur eine Erhöhung der „Quantität“ der staatlichen Souveränität, sondern auch eine wesentliche

Steigerung ihrer „Qualität“. Die Datenhoheit basiert auf der Kontrolle und Nutzung von Daten als neue Art von Ressourcen durch den Staat, während die Cyber-Souveränität mehr auf souveränen Rechten beruht und nicht nur die Beherrschung der Internet- und Informationstechnologie, sondern auch das Recht auf Besitz und Verwaltung von Daten im Cyberspace erfordert (Shi Yuhang 2018). Der Datenfluss beeinflusst die Ausübung der Datenhoheit, während die Kontroll- und Verwaltungsfähigkeit der Datenhoheit für den Datenfluss wiederum Einfluss auf die Ausübung der Cyber-Souveränität nimmt.

Der Vorschlag des Konzepts der Datensouveränität ist angesichts des massiven globalen Datenflusses ein unvermeidlicher Trend für alle Länder der Welt und verkörpert die neuen Änderungen, die der Aufstieg der Technologien wie das Internet, Big Data, künstliche Intelligenz usw. mit sich gebracht hat. Basierend auf den Ansichten von Experten und Wissenschaftlern im In- und Ausland gibt es Datenhoheit im engeren Sinne und Datenhoheit im weiteren Sinne. „Im engeren Sinne bezieht sich die Datenhoheit nur auf die nationale Datenhoheit, während die persönliche Datenhoheit als Datenrechte bezeichnet werden kann, die sich auf das Recht auf Selbstbestimmung und Selbstkontrolle über die persönlichen Daten der Benutzer beziehen“ (Cai Cuihong 2013). Laut Prof. Joel Kinnaman von der Tufts University in den USA umfasst die Datensouveränität im weiteren Sinne die nationale Datensouveränität und die persönliche Datensouveränität. Die nationale Datenhoheit ist Voraussetzung für Verwirklichung der persönlichen Datensouveränität, während die nationale Datenhoheit wiederum von der Unterstützung und dem Ausdruck der persönlichen Datensouveränität abhängt.

Die Datensouveränität ist die Erweiterung der staatlichen Souveränität im Cyberspace. Mit der rasanten Entwicklung der Technologie haben die Informationen über die Grundbedürfnisse der Menschen wie Kleidung, Essen, Wohnen und Verkehr sowie über Politik, Wirtschaft, Kultur und andere Aspekte eines Landes die Form von Daten angenommen. Als unverzichtbare Ressourcen im Zeitalter von Big Data machen Daten einen wachsenden Anteil an allen verfügbaren Ressourcen aus, was einen wichtigen Einfluss auf die Ausweitung der staatlichen Souveränität hat. Die staatliche Souveränität beschränkt sich nicht mehr auf den realen Umfang

des Hoheitsgebiets, des Territorialgewässers, des territorialen Luftraums und der Energie usw. Der aus Daten zusammengesetzte virtuelle Raum erweitert den Darstellungsumfang der staatlichen Souveränität erheblich. Im Cyberspace finden die Verbreitung, der Austausch und die Replikation von Daten anwendbare Grundsätze im Artikel über „Hoheitsrechte“ im „Übereinkommen über den Festlandsockel“. Souveränität und souveräne Rechte stehen in engem Zusammenhang miteinander und sind untrennbar miteinander verbunden. Die Datensouveränität ist nicht nur die Verkörperung höchster souveräner Rechte, sondern auch eine Manifestation der staatlichen Souveränität. Daher soll die Definition der Datensouveränität das traditionelle Konzept der Souveränität nicht loswerden, sondern die staatliche Souveränität als Grundlage nehmen und als Erweiterung der Konnotation der staatlichen Souveränität dienen.

(III) Eigenschaft der Datenhoheit

1. Zeitgenossenschaft

Jede Ära hat eine Reihe von Konzepten, die einzigartig sind, und die Ausweitung des Inhalts der staatlichen Souveränität soll mit der Entwicklung der Zeit Schritt halten. Der Aufstieg des Konzepts der Datenhoheit ist die realistische Grundlage und praktische Anforderung der gegenwärtigen Ära von Big Data. Die staatliche Souveränität soll sich mit der Zeit weiterentwickeln, ihre Epitaxie stets erweitern und die Konnotation bereichern, um die möglicherweise auftretenden komplexen Probleme zu entdecken und zu lösen. Nur wenn wir die Zeitgenossenschaft der Datensouveränität erfassen und die Datensouveränität stets auf dem neuesten Stand halten, können wir den massiven grenzüberschreitenden Datenfluss kontrollieren, die Forderungen nach einer zeitnahen Analyse massiver Daten befriedigen und in der Debatte über die staatliche Souveränität in der Ära von Big Data unbesiegbar sein. Die Zeitgenossenschaft der Datenhoheit bestimmt ihre Entstehung mit dem Herannahen der Ära von Big Data und existiert mit der Existenz der Ära von Big Data zusammen und entwickelt sich mit dieser Ära von Big Data gemeinsam

weiter. Die Datenhoheit ist nie außerhalb unserer Zeit. Stattdessen ist sie ein reales Markenzeichen der Zeit und bewegt sich mit der Zeit vorwärts. Die Datenhoheit basiert auf Technologie, was den Merkmalen der Zeitgenossenschaft entspricht. Im Wesentlichen ist das Vorbringen der Datenhoheit das unvermeidliche Ergebnis einer ausgereiften Datentechnologie. Die Wahrung der Datensicherheit und das Datenressourcenmanagement hängen stark von der Technologie ab. Um die Datenhoheit auszuüben und aufrechtzuerhalten, müssen wir uns auch weitgehend auf die Technologie verlassen. Die Entwicklung der Datenhoheit kann nicht vom Fortschritt in Wissenschaft und Technologie getrennt werden. Die Entwicklung der Wissenschaft und Technologie bestimmt die Ausbreitung des Begriffs, der Konnotation und des Umfangs der Datenhoheit usw. die technologische Innovation und Reife sind Grundlage für Bildung und Entwicklung der Theorie der Datenhoheit und die notwendige Voraussetzung für Ausübung der Datenhoheit.

2. Relativität

Im Zeitalter von Big Data geht die Datenhoheit nur auf Kosten der notwendigen Kompromisse, daher ist sie eine relative Hoheit. Die staatliche Souveränität hat irreversible natürliche Regelmäßigkeit. Sie ist nach innen absolut und nach außen einschränkend, was Relativität darstellt. Die Relativität der Souveränität ist bis zu einem gewissen Grad gerechtfertigt und in der heutigen internationalen Gesellschaft auch generell akzeptiert. Bei der Relativität der Datenhoheit sieht es jedoch anders aus. Die Relativität der Datenhoheit ist insofern relativ, als das akademische Verständnis ihres Konzepts sehr unterschiedlich ist und auch realistische einschränkende Faktoren bestehen. Derzeit ist die Verwirklichung der Datenhoheit horizontalen und vertikalen Einschränkungen ausgesetzt. Die Horizontalen Einschränkungen ergeben sich aus dem Verhältnis der Stärke eines Landes im Cyberspace mit der der anderen Länder, während vertikale Einschränkungen die Machtbeziehungen zwischen den nationalen Staaten, überstaatlichen Ländern, Subländern und sogar bis auf Einzelpersonen im Datenraum bedeuten (Cai Cuihong 2013). Aufgrund der historischen Entwicklung des Konzepts der relativen Souveränität soll

die Souveränität nicht als absolut angesehen werden, sondern soll Einschränkungen unterliegen. Die Relativität der Datenhoheit spiegelt sich in ihrer Definition und ihren Einschränkungsfaktoren wider. Die Definition ihres Begriffs ist sehr verschieden, da es noch keine maßgebliche, klare und einheitliche Definition gibt. Ihre Realisierung hängt von der technologischen Kompetenz des Landes ab. Da die digitale Kluft zwischen Entwicklungs- und Industrieländern in kurzer Zeit wahrscheinlich aber nicht geschlossen werden kann, gibt es daher große Unterschiede zwischen den Landkreisen hinsichtlich der von ihnen erreichten Datenhoheit. Im Cyberspace ist die Kontrolle eines Landes über Datenressourcen relativ, was sich vom absoluten Besitz physischer Ressourcen in der realen Welt unterscheidet. Da der Datenfluss und Datenteilhabe ihren Wert vergrößern und sogar neuen Wert schaffen, sollen Länder die von ihnen besitzenden Datenressourcen unter ihrer Kontrolle teilhaben lassen (Zhu Yanxin 2017).

3. Kooperativität

Die neue Struktur braucht neue Regeln und Mechanismen zu gestalten, um Daten effektiv zu kontrollieren, steuern und zu nutzen. Laut dem amerikanischen Gelehrten Adeno Addis bringt die Datenhoheit zwei widersprüchliche nationale Missionen mit sich: Globalisierung und politische Besonderheit. Die Globalisierung ist eine wichtige Voraussetzung für die Entwicklung und Integration aller Länder in die internationale Gemeinschaft, während die politische Besonderheit dazu dient, die Sicherheit und Interessen verschiedener Länder zu gewährleisten. Die Globalisierung schränkt die Interessen aller Länder gegenseitig ein und führt auch dazu, dass die relevanten Daten aller Länder wechselseitig beeinflussen und voneinander abhängig sind, was ein moderates Maß an Zusammenarbeit erfordert. Die angemessene Zusammenarbeit wird durch die Eigenschaften der Daten selbst bestimmt. Im Allgemeinen haben Daten einen höheren Wert, wenn sie teilgehabt werden. Um globale gemeinsame Interessen zu verfolgen, soll die Zusammenarbeit daher unter der Voraussetzung durchgeführt werden, dass die staatliche Sicherheit und Interessen gewährleistet sind und die Datenhoheit daher

kooperativ ist. Kooperativität bedeutet, dass kein Land allein in der Lage ist, internationale Probleme, die durch Datenhoheit verursacht sind, mit unabhängigen Mitteln zu lösen. Der Schwerpunkt der internationalen Zusammenarbeit in diesem Bereich liegt in der Überwachung und Verteidigung gegen die Hegemonie im Daten-Cyberspace und in gemeinsamen Anstrengungen zum Aufbau eines harmonischen, zivilisierten und schönen Datenraums. „Im Gegensatz zum traditionellen Schutz der Souveränität geht es beim Schutz der Datensouveränität nicht um absoluten Wettbewerb, sondern um Zusammenarbeit in einem gewissen Maß. Da die Daten an sich immateriell sind und problemlos global fließen, ist ein einziges Land nicht in der Lage, nur mit eigener Kraft allein die absolute Kontrolle über Daten zu erlangen, und der Aufbau der absoluten Datenhoheit wäre nichts anderes als ein ‚Luftschloss‘. Es ist für uns viel realistischer, sich beim Aufbau eines Systems der Datenhoheit von der ‚Theorie der relativen Souveränität‘ geleitet zu werden“ (Xiao Dongmei & Wen Yuheng 2017). Die Verwirklichung der Datenhoheit erfordert nicht nur die Unterstützung durch Gesetze, die durch internationale Konsultationen und Konsens erlassen werden, sondern auch die Überwachung durch einschlägige internationale Verträge und Organisationen mit verschiedenen Gerichtsbarkeiten.

4. Gleichheit

Als ein Anspruch bedeutet Gleichheit der Datensouveränität, dass es keine andere externe Autorität als das Völkerrecht geben soll, um über interne Datenangelegenheiten souveräner Staaten zu entscheiden, dass voneinander unabhängige souveräne Staaten die Gleichheit der Datensouveränität füreinander anerkennen und unabhängig voneinander interne Datenangelegenheiten verwalten. Die Gleichheit der Datensouveränität zeigt sich hauptsächlich in der auswärtigen Souveränität eines souveränen Staates. Innerhalb eines Landes spiegelt sich die Datenhoheit in den hierarchischen Beziehungen zwischen der Regierung und ihren untergeordneten Einheiten eines souveränen Staates wider. Nach außen bedeutet Souveränität die Anerkennung eines Landes als politische Einheit durch andere ähnliche Länder, wodurch eine formelle

und gleichberechtigte Beziehung ohne Recht oder Verpflichtung zur Erteilung oder Befolgung von Anweisungen und Befehl zwischen ihnen hergestellt wird. Die souveränen Staaten haben die Macht, ihre eigenen Daten in sich selbst zu besitzen, zu verwalten und zu nutzen, und nach außen haben sie das Recht, Daten vertraulich zu behandeln und Unabhängigkeit und Selbstständigkeit zu wahren. Gleichzeitig sollen sie die Daten anderer Länder respektieren und sich nicht darin einmischen und sie nicht stehlen, was nicht nur die Eigenforderung der Länder, sondern auch ein internationaler Konsens ist. Theoretisch haben alle Länder im Cyberspace die gleiche Datenhoheit. In der Realität besteht jedoch eine große Lücke zwischen Entwicklungs- und Industrieländern hinsichtlich des Niveaus der Datentechnologie, was zu einem großen unterschiedlichen Einfluss im Cyberspace führt, außerdem treiben einige Länder dazu noch Datenhegemonie. Diese zusammen machen es fast unmöglich, theoretische Gleichheit zu realisieren. Infolgedessen ist die Datenhoheit nur förmlich gleich, d.h. die internationalen Vorschriften und Konsens sind nur auf dem Papier und im Bewusstsein, in der Realität aber nicht wirklich umgesetzt. Um die Gleichheit der Datenhoheit im eigentlichen Sinne zu erreichen, müssen wir internationale Vorschriften praktisch umsetzen, internationale Standards einhalten und unbegründete Diskriminierung beseitigen.

Abschnitt II Rechtsposten der Datensouveränität

Nach der traditionellen Theorie ist die staatliche Souveränität die natürliche oberste herrschende Macht innerhalb eines Landes und die Macht, extern unabhängig zu bleiben. Sie umfasst das Zuständigkeitsrecht, das Selbstverteidigungsrecht, das Recht auf Unabhängigkeit, das Recht auf Gleichheit und so weiter. Mit Erstreckung und Erweiterung in den Datenraum umfasst die Datenhoheit auch vier Grundrechte, sie sind: Datenzuständigkeit, die bedeutet, dass ein Staat das Recht hat, seine Daten zu verwalten und zu verfügen; das Recht auf Unabhängigkeit über Daten bezieht sich auf die Unabhängigkeit des Staates bei der Formulierung von

Datengesetzen und -richtlinien und Bestimmung des Datenverwaltungsmodus. Das Recht auf Gleichheit über Daten bedeutet, dass ein Staat keine Zuständigkeit für Daten eines anderen Landes beanspruchen darf und das Recht hat, an der internationalen Zusammenarbeit und Teilhabe an Daten gleichberechtigt teilzunehmen. Das Selbstverteidigungsrecht auf Daten bedeutet, dass ein Staat das Recht hat, Widerstand zu leisten, wenn er Datendiebstahl, -überwachung oder -angriff von außen ausgesetzt ist.

(1) Datenzuständigkeit

Das wichtigste Recht, das ein souveräner Staat intern ausübt, ist das staatliche Zuständigkeitsrecht. Ihr Geltungsbereich deckt natürlich das neue Gebiet der staatlichen Souveränität ab – den Datenraum. Das Zuständigkeitsrecht auf Daten manifestiert sich in der Regulierung des Datenraums durch die nationale Machtbehörde, was das Prinzip der Souveränität konkret widerspiegelt. Wie die Zuständigkeit für andere Elemente ist auch die Datenzuständigkeit ein Teil der nationalen hoheitsrechtlichen Befugnisse. Die Zuständigkeit für Daten ergibt sich daher auch aus der staatlichen Souveränität. Die sogenannte Datenzuständigkeit bezieht sich auf das Recht eines Landes, seine physischen Geräte und damit verbundenen Dienstleistungen zur Datengenerierung, -speicherung und -übertragung zu warten, verwalten und zu nutzen (Cai Cuihong 2013). Im Vergleich zur traditionellen Zuständigkeit wird das Datenzuständigkeitsrecht auch von Personen ausgeübt, die die traditionellen nationalen hoheitsrechtlichen Befugnisse ausüben, während die Objekte des Datenzuständigkeitsrechts Personen oder Organisationen sind, die Daten zur Durchführung verschiedener Aktivitäten und zur Kommunikation verwenden, sowie das Eigentum in ihrem Besitz. Darüber hinaus ist die gesetzliche Hauptgrundlage für Ausübung der Datenzuständigkeit das traditionelle Zuständigkeitsprinzip sowie einige Hilfsprinzipien, die sich aus der Einzigartigkeit der Daten ergeben. Die Zuständigkeit für Daten ist die gleiche wie sie für die traditionelle Zuständigkeit, da sich die Art und Weise ihrer Ausübung und der Inhalt gemäß den einschlägigen Gesetzen

verschiedener Länder einander stark unterscheiden. Wie ein Land sein Datenzuständigkeitsrecht ausübt, hängt von den Bestimmungen seiner Verfassung und denen des internationalen Zuständigkeitsrechts ab (Qi Juxun 2003).

Die Datenzuständigkeit ist eine externe Manifestation der staatlichen Souveränität, und die Relativität der staatlichen Souveränität bestimmt die Relativität der Datenzuständigkeit. Die Relativität der staatlichen Souveränität spiegelt sich in Einschränkungen bei der Ausübung der souveränen Rechte eines Landes sowie in der gegenseitigen Abhängigkeit und Einschränkung zwischen Ländern in Bezug auf die Souveränität wider. Gerade aufgrund der Wechselwirkungen zwischen verschiedenen souveränen Ländern bleibt die Souveränität der Länder erhalten. Mit der tief gehenden wirtschaftlichen Globalisierung nehmen die gegenseitige Abhängigkeit und Interaktion zwischen allen Ländern der Welt zu, und die globalen Probleme vermehren sich auch immer. Kein Land kann isoliert existieren und sich alleine entwickeln, denn der Umweltschutz, Klimawandel, oder internationale Finanzen, Energie- und Ernährungssicherheit usw. sind alles Probleme, mit denen sich kein Land allein befassen kann. Gerade weil diese Kontakte immer tiefer gehen, müssen sich die Länder zusammenschließen und zusammenarbeiten, um Schwierigkeiten gemeinsam zu überwinden und Probleme des Überlebens und der Entwicklung zu lösen.

Ähnlich wie beim traditionellen Zuständigkeitsrecht wird die Datenzuständigkeit in der internationalen Praxis auch von souveränen Staaten praktiziert, die im Allgemeinen den traditionellen Grundsätzen der nationalen Zuständigkeit folgen, nämlich der Grundsatz der hoheitsgebietsbezogenen Zuständigkeit, der Personalitätszuständigkeit, der Schutzzuständigkeit und der universellen Zuständigkeit. Die territoriale Zuständigkeit ist unter anderem die Grundlage der Unabhängigkeit sowie ein unverzichtbares Recht eines Landes. Gemäß dem Grundsatz der territorialbezogenen Zuständigkeit hat ein Staat das Recht, die Zuständigkeit für Personen und ihre Handlungen für Datenübertragung in seinem Hoheitsgebiet auszuüben. Der Grundsatz der Personalitätszuständigkeit, auch als internationale Zuständigkeit bezeichnet, sieht vor, dass ein Staat für seine eigenen Bürger zuständig ist, unabhängig davon, ob sie sich innerhalb oder außerhalb seiner Grenzen befinden, und auch für bestimmte Fälle, in

denen sein Staatsbürger bestimmte Straftaten außerhalb des Landes begeht. Die Schutzzuständigkeit gilt für Situationen, in denen Bürger anderer Länder die Interessen des Landes außerhalb seines Hoheitsgebiets verletzen. Die Voraussetzung dafür ist, dass diese Handlung nicht von Bürger des Landes begangen wurde und auch außerhalb des Hoheitsgebiets des Landes stattfindet, jedoch schwerwiegende verletzende nachteilige Folgen für das Land gebracht hat. Hier hat das geschädigte Land das Recht, die Gerichtsbarkeit über die Bürger eines anderen Landes außerhalb seiner Grenzen auszuüben. Die universelle Zuständigkeit bezieht sich auf das Recht jedes souveränen Staates, die Gerichtsbarkeit für bestimmte spezifische Handlungen auszuüben, die im Allgemeinen den Frieden und die Sicherheit der Menschheit gefährden oder die Stabilität und Ordnung der internationalen Gemeinschaft beeinträchtigen. Der Anwendungsbereich der universellen Gerichtsbarkeit ist relativ begrenzt. Auch wenn dies im grenzüberschreitenden Datenfluss geschieht, muss sie auch nur auf der Grundlage expliziter völkerrechtlicher Bestimmungen erfolgen.

In der internationalen Gesellschaft werden Gerichtsbarkeitsstreitigkeiten zwischen Ländern in Bezug auf einige internationale Angelegenheiten häufig durch ein gemeinsam ausgehandeltes Abkommen oder durch den Internationalen Gerichtshof oder andere ähnliche Mittel beigelegt. Im Prozess der Behandlung internationaler Streitigkeiten hat der geografische Ort, an dem Streitigkeiten auftreten, häufig wichtige Auswirkungen und kann in bestimmten Situationen sogar eine Schlüsselrolle spielen. Im Datenraum ist es jedoch schwierig, den Ort und die Zeit einer Streitigkeit zu definieren. Das heißt, die traditionelle Zuständigkeit gilt möglicherweise nicht für den Datenraum. Daher ist es dringend erforderlich, dass wir so bald wie möglich spezielle Zuständigkeitsregeln für den Datenraum erstellen. Im Zeitalter von Big Data wird die nationale Gerichtsbarkeit häufig von einigen Datenbürgern ignoriert. Sie glauben, dass sie in einem Raum ohne Einschränkungen existieren und alles tun können, was sie wollen. Da der Datenraum virtuell, global und grenzenlos ist, führt es oft dazu, dass sich die Bereiche der Datenzuständigkeit verschiedener Länder wahrscheinlich überschneiden, was die gerichtliche Tätigkeit eines Landes für seine eigenen Angelegenheiten mittelbar beeinflusst und mehr Schwierigkeiten für die justizielle Operation dieses Landes bringt. So ist eine engere

Zusammenarbeit und Koordinierung zwischen verschiedenen Ländern im Datenraum erforderlich. Die besonderen Merkmale des Datenraums haben oft zu Rückschlägen bei der Ausübung der nationalen Gerichtsbarkeit geführt, während die Einschränkungen der traditionellen Gerichtsbarkeit im Zeitalter von Big Data allmählich sichtbar werden. Insbesondere ist es schwierig, das Prinzip der territorialen Zuständigkeit der realen physischen Welt direkt auf den virtuellen Datenraum anzuwenden. Für die Personalitätszuständigkeit ist die Identität der Datennutzer schwer zu bestimmen. Die Anwendung der Schutzgerichtsbarkeit ist auch mit verschiedenen Hindernissen im Datenraum konfrontiert, während die Durchführung der universellen Gerichtsbarkeit im Datenraum auch mehrere Mängel zeigt, deren Gründe wahrscheinlich nicht einzeln aufgeführt werden können.

(II) Unabhängigkeitsrecht auf Daten

Das Recht auf Unabhängigkeit ist der grundlegendste Teil der staatlichen Souveränität. Dies bedeutet, dass „ein Land seine Macht unabhängig und vollständig ohne ausländische Einmischung oder Einschränkung durch andere Länder ausüben kann“ (Xie Yongjiang 2018). Artikel 2 Absatz 7 der „Charta der Vereinten Nationen“ bestimmt: „Nichts in dieser Charta berechtigt die Vereinten Nationen, in Angelegenheiten einzugreifen, die im Wesentlichen in die innerstaatliche Zuständigkeit eines Staates fallen ... aber dieser Grundsatz berührt nicht die Anwendung von Durchsetzungsmaßnahmen nach Kapitel VII.“ Das Ziel ist es, die Unabhängigkeit der staatlichen Souveränität gegenüber der Außenwelt zu betonen und kein Land oder keine Organisation hat das Recht, sich aus irgendwelchem Grund in die Angelegenheiten anderer Länder einzumischen. Nach der „Charta der Vereinten Nationen“ nahm die Generalversammlung der Vereinten Nationen 1965 die „Erklärung über die Unzulässigkeit von Eingriffen in die inneren Angelegenheiten der Staaten und den Schutz ihrer Unabhängigkeit und Souveränität“ an (im Folgenden als Erklärung bezeichnet). In dieser Erklärung wird weiter betont, dass die Unabhängigkeit der staatlichen Souveränität geschützt wird und dass die Außen- und Innenangelegenheiten eines Landes vom Land selbstständig

behandelt und verwaltet werden müssen. Gleichzeitig darf sich kein Staat in irgendeiner Form in die inneren Angelegenheiten anderer Länder einmischen oder diese behindern, kein Staat darf sich aus irgendeinem Grund direkt oder indirekt an den inneren Unruhen anderer Länder beteiligen, und kein Staat darf Aktivitäten zur Untergrabung der Regierung in anderen Ländern organisieren, unterstützen, fördern, anstiften, finanzieren, anregen oder tolerieren. Die Länder sollen gegenseitigen Respekt vor der souveränen Unabhängigkeit haben. Dementsprechend besteht das Hauptziel des Rechts auf Unabhängigkeit darin, dass jedes Land seine externen und internen Angelegenheiten unabhängig und selbstständig nach eigenem Willen ohne jegliche Kontrolle und Einmischung anderer Länder abwickeln kann.

Die staatliche Souveränität „impliziert daher eine umfassende Unabhängigkeit innerhalb und außerhalb der Landesgrenzen“ (Jennings & Watts 1995, S. 92). Im Zeitalter von Big Data sollen souveräne Staaten auch unabhängig sein, um Macht im Datenraum auszuüben. Das sogenannte Unabhängigkeitsrecht auf Daten bedeutet, dass ein Land das Recht hat, die Dateninfrastruktur und -ressourcen innerhalb des Landes unabhängig zu verwalten, die Datensicherheit des Landes zu schützen und zu verhindern, dass andere Länder willkürlich in seine Dateninfrastruktur und -ressourcen eingreifen. Das Recht auf Unabhängigkeit über Daten umfasst zunächst das Recht souveräner Staaten, ihren eigenen Datenraum zu regeln. Das Recht auf Regulierung kann viele Formen annehmen, wie moralische Regeln, Richtlinien und Gesetze etc., vor allem um die oberste Autorität des Landes im Datenraum aufrechtzuerhalten. Zweitens beinhaltet es das Recht, Eingriffe anderer Länder in die Datenverwaltung zu verbieten. Obwohl es im Datenraum keine Grenzen gibt, soll die Datenverwaltung eines Landes nicht von anderen Ländern zwingenderweise gestört werden. Der feste Widerstand gegen die Datenhegemonie ist ein wirksames Mittel, um die Unabhängigkeit der Datenhoheit aller Länder aufrechtzuerhalten (Jiang Ruihao 2016).

Das Verhältnis zwischen dem Datenunabhängigkeitsrecht und dem traditionellen Recht auf nationale Unabhängigkeit wird wie folgend beschrieben. Zuerst ist das Datenunabhängigkeitsrecht die Entwicklung und Erweiterung des Unabhängigkeitsrechts in der traditionellen Theorie der

nationalen Souveränität. Als Anwendung des nationalen Unabhängigkeitsrechts im Datenraum bestätigt und verfolgt die Datenunabhängigkeit nicht nur den Zweck und die Elite der traditionellen Theorie der nationalen Unabhängigkeit, sondern bereichert und entwickelt auch die traditionelle Theorie der nationalen Souveränität und verleiht ihr ständig Aura unserer neuen Ära und tiefe Konnotation. Zweitens ist das traditionelle nationale Unabhängigkeitsrecht die theoretische Grundlage des Datenunabhängigkeitsrechts. Wie das Hauptziel des traditionellen Unabhängigkeitsrechts befolgt das Datenunabhängigkeitsrecht den Geist des Grundsatzes „Nichteinmischung in innere Angelegenheiten“, entspricht den Bestimmungen des Völkerrechts für das Unabhängigkeitsrecht und stimmt mit den Entwicklungstrends der internationalen Gemeinschaft und des Völkerrechts auch überein. Schließlich sind das Datenunabhängigkeitsrecht und das nationale Unabhängigkeitsrecht in einer dialektischen Einheit. Sie beiden sind zwei Dimensionen der Entwicklung derselben Sache. Die Anwendung des nationalen Unabhängigkeitsrechts im Datenraum wird mit einigen Herausforderungen verbunden, die es unmöglich machen, die Entwicklung der laufenden internationalen Beziehungen im Zeitalter von Big Data weiter anzupassen. Verglichen mit dem Recht auf nationale Unabhängigkeit ist das Datenunabhängigkeitsrecht im Zeitalter von Big Data besser an die Umgebung im In- und Ausland des Datenraums im Zeitalter von Big Data angepasst.

Das Datenunabhängigkeitsrecht setzt voraus, dass das Datensystem eines Landes, einschließlich sogar seines Netzwerks und seiner Anwendungstechnologie, keinen Beschränkungen eines anderen Landes oder einer anderen Organisation unterliegt. Unter dem Gesichtspunkt der Auflösung von Domainnamen hängt der derzeitige Betrieb des Internets in verschiedenen Ländern jedoch stark vom Stammmamenserver ab, der sich in den USA befindet. Dies wirkt sich bis zu einem gewissen Grad auf die Ausübung des Datenunabhängigkeitsrechts aus. Das System von Domain Name Resolution übernimmt ein „zentrales und hierarchisches Verwaltungsmodell“. In diesem Modell gibt es zwei Hauptrisiken bei der Auflösung von Domainnamen: Erstens können inländische Domainnamen blockiert werden. Wenn der Registrierungsdatensatz des Top-Level-Domainnamens eines Landes nur vom ursprünglichen Root-Nameserver gelöscht wird,

kann kein Benutzer eines anderen Landes unter den Domainnamen dieses Landes auf die Websites zugreifen. Unter diesen Umständen wird auch das mehrstufige System zur Auflösung von Domänennamen völlig zusammenbrechen. Zweitens ist das Risiko, nicht auf das Internet zugreifen zu können. Solange der ursprüngliche Root-Nameserver und alle seine Slave-Server und Image-Server die Bereitstellung von Root-Name-Diensten für die IP-Adressen aller rekursiven DNS-Server in einem Land verweigern, haben die Internetbenutzer, die sich auf rekursive DNS-Server dieses Landes verlassen, keinen Zugriff auf das Internet, da sie keine Dienste zur Auflösung von Domainnamen erhalten können (Fang Binxing 2014).

Laut Statistik gibt es derzeit weltweit 13 Internet-Root-Server, von denen sich der einzige primäre Root-Server in den USA befindet und neun der übrigen 12 sekundären Root-Server sich ebenfalls in den USA befinden. Es ist ersichtlich, dass die Vereinigten Staaten die Kontrolle über die Kern- und Schlüsselgrundressourcen des globalen Internets haben. Sobald der Domain-Name eines Landes auf dem Root-Server blockiert ist, können alle Websites unter diesem Top-Level-Domain-Namen sofort aus dem Internet „verschwinden“. In diesem Sinne haben die Vereinigten Staaten die einzigartige Datenherrschaft, an der kein anderes Land messen kann, und können die Datenhoheit anderer Länder abschrecken. Es ist auch ersichtlich, dass kein Land außer den Vereinigten Staaten vollständige Unabhängigkeit über seine Daten im Internet hat. Um das Datenunabhängigkeitsrecht im Cyberspace für alle Länder zu verwirklichen, muss die Verwaltung des Root-Servers des Internets an eine internationale Organisation wie die Vereinten Nationen übertragen werden. China hat sich seit Langem dazu verpflichtet, die Vereinten Nationen aufzufordern, die Kompetenzarbeit des Internet-Namenmanagements und der Agenturen für die Verteilung digitaler Adressen zu übernehmen. Nachdem die internationale Gemeinschaft jahrelang Druck ausgeübt hatte, übertrug die National Telecommunication and Information Administration, eine Tochtergesellschaft des US-Handelsministeriums, am 1. Oktober 2016 schließlich die Verwaltungsbefugnis der Agentur für die Verbreitung digitaler Internetadressen an die Internet Name und digitale Adresse Vertriebsagentur in Kalifornien und beendete den Autorisierungsverwaltungsvertrag zwischen den beiden. Die Übertragung der Verwaltungsbefugnis von Agenturen für

die Verteilung digitaler Internetadressen wird den Ländern objektiverweise helfen, die Kontrolle in Bezug auf Cyberdaten von den Vereinigten Staaten loszuwerden und unabhängiger zu werden (Huang Zhixiong 2017, S. 146).

(III) Recht auf Datengleichheit

„Als Grundwert für den Aufbau einer soliden sozialen Ordnung ist die Gleichheit das, was die Menschheit seit der Geburt der menschlichen Gesellschaft verfolgt“ (Wu Shan & Liu Yading 2010). Das Recht auf Gleichheit ist „legalisierte und standardisierte Gleichheit, die eine bessere Ordnung darstellt“ (Wang Xiangrong 2019). Aus der Perspektive der Beziehungen zwischen Ländern ist das Recht auf Gleichheit eines der Grundrechte eines Landes und der grundlegende Ausdruck der Souveränität eines Landes. Das Recht auf Gleichheit bezieht sich auf den gleichen Status aller Länder vor dem Völkerrecht, unabhängig von ihrer Stärke oder Größe, ihren politischen oder wirtschaftlichen Modellen, ihrer kulturellen Gedanken, ihrem Sozialsystem und ihrer Ideologie. Im Jahre 1648 legte das „Westfälische Friedensabkommen“ die wichtigen Rechtsgrundsätze der modernen internationalen Beziehungen klar fest und bestätigte den gleichen Status der nationalen Souveränität. Die Anerkennung des Grundsatzes der souveränen Gleichheit im zeitgenössischen Völkerrecht spiegelt sich hauptsächlich in der 1945 verabschiedeten „Charta der Vereinten Nationen“ wider. In der Präambel wird der Glaube an die „Gleichberechtigung ... der großen und kleinen Nationen“ klar zum Ausdruck gebracht. In Artikel 2 Absatz 1 heißt es ausdrücklich: „Diese Organisation basiert auf dem Grundsatz der souveränen Gleichheit aller ihrer Mitglieder.“ Nach Vorschriften des Völkerrechts sind alle Länder, ob groß oder klein, stark oder schwach, gleichberechtigte Mitglieder der internationalen Gemeinschaft. Mit anderen Worten, obwohl es Unterschiede im territorialen Bereich, in der wirtschaftlichen und militärischen Stärke usw. gibt, gibt es keinen Unterschied in Bezug auf ihren rechtlichen Status, ihre gesetzlichen Rechte und andere souveräne Rechte und Interessen. Jedes Land ist vor dem Völkerrecht gleichberechtigt und seine legitimen Rechte und Interessen sind gleich und alle

Länder müssen sich an die Grundnormen des Völkerrechts und der internationalen Beziehungen halten.

Ian Brownlie hat einmal darauf hingewiesen, dass „die Gleichheit der staatlichen Souveränität die grundlegende Verfassungslehre des Völkerrechts ist“. Daraus kann geschlossen werden, wie wichtig das staatliche Gleichheitsrecht für die souveränen Länder ist (Fang Binxing 2017, S. 67–68). Als eines der Grundrechte eines Landes ist das Recht auf Gleichheit eines Landes ein wichtiges Symbol seiner Souveränität. Als natürliche Erweiterung der staatlichen Souveränität im Datenraum im Zeitalter von Big Data soll die Datenhoheit gleich sein. Die Gleichheit der Datensouveränität spiegelt sich hauptsächlich unter den souveränen Ländern wider, d.h. in der externen Souveränität. Die Datenhoheit ist intern die höchste Macht von oben nach unten, während sie extern bedeutet, dass alle souveränen Staaten unabhängig und miteinander identifiziert sind. Kein Land darf ein anderes Land aufgrund internationaler Angelegenheiten verwalten. Und es gibt auch keine Rechte und Pflichten zwischen Ländern. Die Beziehungen zwischen den Ländern müssen gleich sein, was auch die gebührende Bedeutung der nationalen Souveränität darstellt. Mit anderen Worten: da ein Staat die Freiheit hat zu erklären, dass er nicht von anderen Staaten innerhalb seiner Souveränität eingeschränkt und kontrolliert wird, muss er auch anerkennen, dass andere Staaten innerhalb ihrer eigenen Souveränität die gleiche Freiheit genießen (Zhang Jingwen 2018, S. 8).

Wie das Recht auf nationale Gleichheit ist das Datengleichheitsrecht auch ein wichtiges Symbol für die Datenhoheit. Das sogenannte Datengleichheitsrecht bedeutet, dass „ein Land keine Datenzuständigkeit gegenüber anderen Ländern und die gleichen Rechte zur Teilnahme an der internationalen Zusammenarbeit und Teilhabe an Daten beanspruchen darf“ (Li Aijun & Zhang Jun 2017, S. 34). Das Datengleichheitsrecht erfordert, dass die wichtige Bedeutung von Daten von der internationalen Gemeinschaft akzeptiert wird und dass die Datensouveränität zu einem wichtigen Bestandteil der nationalen Souveränität gemacht wird, um den gleichberechtigten Austausch von Teildaten zu verwirklichen und den Ländern zu ermöglichen, das Recht auf Gleichheit beim Datenaustausch in der internationalen Gemeinschaft zu genießen. In der Praxis umfasst das Datengleichheitsrecht folgende Aspekte: Erstens ist die Gleichheit der

Datenressourcen. Die Datenressourcen sind der gemeinsame Reichtum der gesamten Menschheit, und die Bevölkerung in jedem Land hat das Recht, Daten ohne Diskriminierung frei zu verwenden unter der Voraussetzung, dass sie die Interessen anderer Länder und Völker nicht verletzen. Zweitens ist die Gleichheit, Datenregeln zu erstellen. Alle Länder haben nicht nur das gleiche Rederecht im globalen Datenverwaltungssystem, sondern sollen auch vermeiden, die Interessen von Ländern verletzt zu werden, von deren Datendiensten diese Länder abhängig sind, wenn sie ihre eigenen Datenregeln festlegen. Die Ungleichheit bei der Festlegung von Datenregeln wird zwangsläufig dazu führen, dass einige Länder von den Industrieländern ungleich behandelt werden. Schließlich soll das Datengleichheitsrecht auch die Immunität des staatlichen Verhaltens im Datenraum betonen, die eine Fortsetzung der traditionellen Theorie der staatlichen Immunität im Zeitalter von Big Data darstellt und die Gleichheit der nationalen Souveränität mittelbar widerspiegelt.

Das Datengleichheitsrecht ist relativ, was durch die Datenverarbeitungsfähigkeit jedes Landes bestimmt wird. Angesichts der rasanten Entwicklung von Wissenschaft und Technologie muss die internationale Gemeinschaft die Zusammenarbeit stärken und beschleunigen und einheitliche Regeln für den Datenraum festlegen, um die gesetzlichen Verschiedenheiten zwischen den Ländern zu beseitigen und die Schaffung einer neuen globalen Datenraumordnung zu fördern. Das Datengleichheitsrecht betrifft nicht nur die direkte Gleichheit anfänglich bei der Zuweisung von Datenressourcen, sondern auch die gleiche Fähigkeit, Ressourcen nach der Zuweisung von Datenressourcen zu transformieren. Die bestehende Realität ist jedoch, dass die Entwicklungsländer bei der Entwicklung der Datentechnologie weit hinter den Industrieländern zurückliegen und einen relativ kleineren Einfluss auf den Datenraum haben. Dazu verhalten sich einige Industrieländer im Datenraum noch hegemonial, sodass eine vollständige Gleichstellung vorerst grundsätzlich nicht möglich ist. Beispielsweise sind viele Entwicklungsländer aufgrund ihrer begrenzten technologischen Kapazität nicht in der Lage, Daten sicher zu speichern und zu verarbeiten, sie können nichts anderes als ihre Daten nur an Industrieländer übertragen und müssen sogar das hegemoniale Verhalten dieser Länder erleiden.

Das Hauptproblem des Datengleichheitsrechts ist das Fehlen der Datengleichheit in verschiedenen Ländern. Gegenwärtig ist der Entwicklungsstand der Datentechnologie in verschiedenen Ländern der Welt uneinheitlich, und es besteht Ungleichheit, wenn Länder ihre Rechte im Bereich Big Data ausüben. Einerseits haben die Vereinigten Staaten und andere Industrieländer eine absolute Vorherrschaft in der Datentechnologie, während sich die Mehrheit der Entwicklungsländer in einer benachteiligten Position befindet. Andererseits ist die Fähigkeit zum Sammeln, Speichern, Übertragen, Verarbeiten und Verwenden von Daten aufgrund der großen Unterschiede in den technologischen Fähigkeiten verschiedener Länder nicht dieselbe, was zu einem Ungleichgewicht im Prozess des grenzüberschreitenden Datenflusses führt. Aufgrund der Liquidität und Aktualität des grenzüberschreitenden Datenflusses ist es leichter, Daten in Industrieländer zu fließen, die über mehr Kapital und Ressourcen verfügen. Die Beherrschung massiver Datenressourcen erleichtert es wiederum den Industrieländern, ihre datenbezogenen Vorteile zu erweitern, die Kluft zwischen ihnen weiter zu vergrößern und die industrielle Souveränität und wirtschaftlichen Entwicklungsmöglichkeiten weniger entwickelter Länder zu nutzen. Dies wird zu weiteren Verlusten der Gleichberechtigung führen. Daher soll die internationale Gemeinschaft das Konzept der Gleichheit in der Datensouveränität energisch fördern. Um eine gleichmäßige Verteilung der Dateninteressen zu erreichen, kann man aus dem Gesetzgebungskonzept des „Prinzips der gemeinsamen Interessen der ganzen Menschheit“ im „Weltraumvertrag“ lernen und es als Beispiel nehmen, damit alle Länder der Welt die enormen Vorteile des Datenraums nutzen können und alle Länder der Welt das gleiche Sprechrecht und Beteiligungsfähigkeit bei der globalen Datenverwaltung haben und zusammenarbeiten, um ein für beide Seiten vorteilhaftes Gewinn-Gewinn-Modell für die Datenverwaltung zu entwickeln.

(IV) Recht auf Datenselbstverteidigung

Das Recht auf Selbstverteidigung ergibt sich aus der nationalen Souveränität. Nach dem Prinzip der nationalen Souveränität sind alle Länder

verpflichtet, die Souveränität und Unabhängigkeit anderer Länder zu respektieren. Alle Länder haben das Recht, alle nach internationalem Recht zulässigen Maßnahmen zur Selbsterhaltung zu ergreifen, um ihr Überleben und ihre Sicherheit zu gewährleisten und ihre Souveränität und Unabhängigkeit zu wahren. Im traditionellen Völkerrecht besitzt ein Land das Recht auf Krieg, sodass es seine eigenen Rechte und Interessen mit verschiedenen Maßnahmen, einschließlich des Krieges, erlangen oder aufrechterhalten kann, um Selbsterhaltung und Selbstentwicklung zu verwirklichen. In diesem Sinne ist das Recht auf Krieg ein wichtiger Bestandteil des Rechts auf Selbsterhaltung eines Landes nach dem traditionellen Völkerrecht. 1928 erklärte die Unterzeichnung „des Nichtkrieg-Paktes von Paris“ erstmals den Krieg für illegal. Nach dem Zweiten Weltkrieg, als die „Charta der Vereinten Nationen“ in Kraft trat, hob das moderne Völkerrecht das Recht auf Krieg eindeutig auf und machte es nicht mehr zu einem legitimen Recht eines Staates, auf diese Weise Selbsterhaltung und Entwicklung zu verwirklichen. Ein solcher Übergang führte zu richtiger Zeit zum Recht auf Selbstverteidigung. Im internationalen Rechtssystem ist das Selbstverteidigungsrecht als Grundrecht eines Landes der nationalen Souveränität untergeordnet. Das nationale Selbstverteidigungsrecht ist hauptsächlich in Artikel 51 der „Charta der Vereinten Nationen“ vorgesehen². Gemäß diesem Artikel besitzt ein Staat das ihm innewohnende Recht, gegen bewaffnete Angriffe zu kämpfen, d.h. das Recht auf Selbstverteidigung.

Das Recht auf Selbstverteidigung bezieht sich auf das Recht eines Staates, den bewaffneten Angriffen externer Kräfte mit Gewalt zu widerstehen,

- 2 Artikel 51 der Charta der Vereinten Nationen lautet: „Nichts in dieser Charta beeinträchtigt das inhärente Recht auf individuelle oder kollektive Selbstverteidigung, wenn ein bewaffneter Angriff gegen ein Mitglied der Vereinten Nationen erfolgt, bis der Sicherheitsrat die erforderlichen Maßnahmen ergriffen hat den internationalen Frieden und die internationale Sicherheit aufrechtzuerhalten. Maßnahmen, die von Mitgliedern zur Ausübung dieses Rechts auf Selbstverteidigung ergriffen werden, sind dem Sicherheitsrat unverzüglich zu melden und berühren in keiner Weise die Befugnis und Verantwortung des Sicherheitsrates gemäß dieser Charta, jederzeit solche Maßnahmen zu ergreifen hält es für notwendig, um den internationalen Frieden und die internationale Sicherheit aufrechtzuerhalten oder wiederherzustellen.“

um sein inhärentes oder natürliches Recht zu wahren. In der internationalen Gemeinschaft gab es seit Langem Streitigkeiten und Debatten über das nationale Selbstverteidigungsrecht, deren Schwerpunkt hauptsächlich auf der Verschiedenheit der Auslegung des Selbstverteidigungsrechts in der Charta der Vereinten Nationen liegt. Zur Definition des nationalen Selbstverteidigungsrechts gibt es zwei Hauptansichten: das nationale Selbstverteidigungsrecht im engeren Sinne und im weiteren Sinne. Im engeren Sinne bezieht sich das nationale Selbstverteidigungsrecht auf das Recht eines Landes, eine separate oder kollektive bewaffnete Selbstverteidigung durchzuführen, um gegen den Angreifer zu kämpfen und sich zu verteidigen, wenn er sich einem externen bewaffneten Angriff ausgesetzt wird (Zhou Gengsheng 1981, S. 77). Im weiteren Sinne ist das nationale Selbstverteidigungsrecht einem Land als internationale Persönlichkeit innewohnend und das Recht eines Landes, seine eigene Existenz und Unabhängigkeit zu verteidigen (Zhang Naigen 2002, S. 95). Das Recht auf Selbstverteidigung, wie chinesische Gelehrte es nennen, bezieht sich gewöhnlich auf das Selbstverteidigungsrecht im engeren Sinne. Sie glauben, dass das Selbstverteidigungsrecht ein natürliches Recht eines Landes ist, das sich aus seiner nationalen Souveränität ergibt. Basierend auf einer Zusammenfassung relevanter Gesichtspunkte soll das nationale Selbstverteidigungsrecht wie folgt definiert werden: Erstens ist es das inhärente Recht eines Staates als internationale Persönlichkeit. Zweitens ist es das Recht, das Überleben und die Unabhängigkeit eines Staates zu verteidigen. Drittens soll der Staat bei der Ausübung des nationalen Selbstverteidigungsrechts keinen Missbrauch des Selbstverteidigungsrechts üben (He Fuyong & Duan Jindong 2005).

Lassa Oppenheim, der berühmte britische Gelehrte des Völkerrechts, glaubte, dass kein Land auf der Grundlage des gebräuchlichen Völkerrechts verpflichtet ist, passiv zu bleiben, wenn ein anderes Land seine gesetzlich geschützten Interessen benachteiligt. Wenn ein Land gewaltsam angegriffen wird, hat es das Recht, bei Bedarf Gewalt anzuwenden, um sich zu verteidigen, die Angreifer abzuwehren und sie aus seinem Hoheitsgebiet zu vertreiben. Bei einem Angriff auf Daten unterscheidet sich das Recht auf Selbstverteidigung gegen einen virtuellen Datenangriff jedoch von dem im allgemeinen Völkerrecht festgelegten Recht auf Selbstverteidigung. Wenn der Datenangriff die Schlüsseldateninfrastruktur eines Landes ernsthaft

beschädigt, hat der verletzte Staat das Recht, sein Recht auf Selbstverteidigung gegen den Angreifer auszuüben, d.h. das Selbstverteidigungsrecht auf Daten auszuüben, wobei aber bestimmte Bedingungen erfüllt werden müssen und Einschränkungen in gewissem Maße unterliegen. Das Selbstverteidigungsrecht auf Daten basiert auf dem traditionellen Recht auf Selbstverteidigung, das zur Wahrung der Datenhoheit eingerichtet wurde. Darüber hinaus ist es ein wichtiges und unverzichtbares Recht eines Landes, seine Datensicherheit und -entwicklung aufrechtzuerhalten. Das Selbstverteidigungsrecht auf Daten bezieht sich auf das Recht eines Landes, seine eigenen Rechte und Interessen zu schützen, wenn seine Datenhoheit einem externen Datendiebstahl, einer Überwachung oder einem Angriff ausgesetzt ist.

Gemäß Bestimmung in Artikel 51 der „Charta der Vereinten Nationen“ muss die Ausübung des Selbstverteidigungsrechts eines Staates auf der Voraussetzung eines bewaffneten Angriffs beruhen, der stattgefunden hat oder bevorsteht. Artikel 51 hat jedoch nur den Begriff „bewaffneter Angriff“ erwähnt, ohne genau zu definieren, was ein „bewaffneter Angriff“ ist, geschweige denn klar definiert, dass ein Datenangriff als bewaffneter Angriff im herkömmlichen Sinne angesehen werden kann. Als eine völlig neue Art von Kriegsführung betrachtet der Datenangriff den physischen Massenschaden nicht als einen wesentlichen Faktor, kann das Kampfkommandosystem des Feindes aufgrund der zunehmenden Abhängigkeit moderner Kriegsoperationsmechanismen von Daten jedoch leicht gestört und zerstört werden und dann die physischen militärischen Einrichtungen, Waffen und Ausrüstungen des Feindes zerstört werden und sogar tödlicher Schaden für die Kombattanten verursacht werden. In gewissem Maße unterscheidet sich ein Datenangriff nicht von den konkreten militärischen Mitteln, die in traditionellen Kriegen eingesetzt werden. Wenn ein Datenangriff dem Angegriffenen einen schweren physischen Schaden zufügt, kann dies als bewaffneter Angriff im Sinne des „Gesetzes über bewaffnete Konflikte“ angesehen werden, und dann können souveräne Staaten ihre Selbstverteidigung gegen einen solchen Datenangriff durchführen und ihr Selbstverteidigungsrecht auf Daten ausüben.

Das Völkerrecht erkennt das natürliche Selbstverteidigungsrecht des Staates an, schränkt aber dessen Ausübung ein. In der Caroline-Affäre

machte der damalige Außenminister der Vereinigten Staaten, Daniel Webster, in seiner Antwort auf die Notiz des britischen Botschafters deutlich, dass ein Staat zwar das Recht auf Selbstverteidigung hat, die Ausübung des Selbstverteidigungsrechts jedoch nur in der Situation beschränkt sein soll, in der es „augenblickliche und überwältigende Dringlichkeit, keine andere Wahl der verfügbaren Mittel und auch keinen Moment für detaillierte Überlegung“ zur Selbstverteidigung gibt (Caroline-Affäre 2019). Ebenso wie die Einschränkungen der Ausübung des staatlichen Selbstverteidigungsrechts wird sich das Selbstverteidigungsrecht auf Daten möglicherweise zu bewaffneten Vergeltungsmaßnahmen entwickeln, wenn notwendige Einschränkungen nicht auf das Maß der Ausübung des staatlichen Datenselbstverteidigungsrechts auferlegt werden. Darüber hinaus verstoßen bewaffnete Vergeltungsmaßnahmen gegen den Zweck des modernen Völkerrechts und sind illegal. Infolgedessen muss die Ausübung des Selbstverteidigungsrechts bestimmten Grenzen unterliegen, nämlich dem Grundsatz der Notwendigkeit und der Verhältnismäßigkeit. Das Notwendigkeitsprinzip zielt hauptsächlich darauf ab, die Mittel und Methoden der Kriegsführung, mit denen der Staat das Selbstverteidigungsrecht auf Daten ausübt und die sofortige Ausübung des Selbstverteidigungsrechts auf Daten zu regeln. Der Grundsatz der Verhältnismäßigkeit verlangt, dass bei der Ausübung des staatlichen Datenselbstverteidigungsrechts eine angemessene Verhältnismäßigkeit zwischen dem Ausmaß der angewandten Gewalt und dem erlittenen Schaden sowie zwischen den spezifischen und direkten militärischen Interessen oder den geschützten Rechten und Interessen die möglichen Kollateralschäden von Zivilisten und zivilen Gegenständen bestehen muss (Gu Dexin 2001).

Abschnitt III Spiel der Datensouveränität

Der Status von Daten als eine Art grundlegende strategische Ressource wird immer wichtiger. Alle Länder sind für ihre wirtschaftliche Entwicklung, ihren Aufbau und ihre soziale Stabilität immer mehr auf Datenressourcen angewiesen. „Der Wettbewerb um Datenressourcen wird immer

heftiger, die Datenhoheit steht im Mittelpunkt des Spiels zwischen mehreren Parteien und der Wettbewerb zwischen Ländern um die Dominanz über Dateninformationen wird immer härter“ (Zhao Gang, Wang Shuai & Wang Peng 2017). In der Praxis führt die absolute Unabhängigkeit der Datensouveränität zu Konflikten mehrerer Zuständigkeitsrechte und Zwangslage der Staatssicherheit, sodass das Spiel und die Konfrontation der Datensouveränität letztendlich zu Störung und Unordnung im Datenraum in der internationalen Gemeinschaft führen. In diesem Hintergrund sollen alle Länder zur souveränen Zusammenarbeit und Beteiligung zurückkehren, um einen Ausweg aus der schwierigen Situation der Unordnung zu finden und eine „gemeinsame Regulierung und Verwaltung“ der Datenraumgemeinschaften zu implementieren, damit der dauerhafte Frieden, die allgemeine Sicherheit und gemeinsame Entwicklung der Menschheit gewährleistet werden.

(I) Konflikte der Datensouveränität

Der grenzüberschreitende Fluss und die Speicherung von Daten haben die traditionelle Theorie der absoluten Unabhängigkeit der Souveränität infrage gestellt. Es ist für einen unabhängigen souveränen Staat unmöglich, das Recht auf Besitz und Zuständigkeit von nationalen Daten ganz selbstständig auszuüben und ausländische Einmischung vollständig auszuschließen. Wenn ein Land eine absolute und einseitige Kontrolle über Daten und verwandte Technologien aufgrund der Unabhängigkeit der Datensouveränität durchführt, führt dies zu einem spontanen Spiel und einer Konfrontation der Datensouveränität und schließlich zu einer Unordnung im Datenraum der internationalen Gemeinschaft. Infolgedessen ist die Überbetonung der Unabhängigkeit der Datensouveränität die Hauptursache für die Konfrontation der Länder wegen der Datensouveränität. Gegenwärtig resultiert das spontane Spiel der Datensouveränität vor allem aus dem Grund des Konflikts mehrerer Zuständigkeitsrechte auf Daten und der Notlage der nationalen Datensicherheit.

Der Konflikt mehrerer Datenzuständigkeitsrechte. Im Zeitalter von Big Data steht das Völkerrecht vor zahlreichen Herausforderungen, von

denen die nachhaltigste und tiefste darin besteht, dass Daten den Gesetzen verschiedener Länder unterliegen, die auf den Orten des Besitzes, der Speicherung und der Übertragung basieren. Gleichzeitig lagern Datenanbieter häufig einen Teil ihrer Dienste aus, um Kosten zu senken und Bedürfnisse der Kunden zu erfüllen. Dann unterliegt dieser Teil der Daten möglichst mehreren Gerichtsbarkeiten, da sie unterschiedliche Länder betreffen, insbesondere weil die Länder den Umfang der Gerichtsbarkeit der Datenhoheit noch nicht klar definiert haben und alle Länder ihre Rechte in der internationalen Gemeinschaft auf völlig rationale Weise ausüben. Bevor ein einheitliches internationales System oder ein Koordinierungsmechanismus eingerichtet wird, beanspruchen alle Länder die Datenhoheit über alle Daten, die sie überwachen können, um die absolute nationale Sicherheit zu gewährleisten und eine ausreichende Überwachung zu erreichen. Dies wird unweigerlich zur Überwachung einiger extraterritorialer Daten führen, wodurch die Situation mehrerer Gerichtsbarkeiten gebildet wird. Insgesamt haben die derzeitigen Praktiken, die auf der Betonung der Unabhängigkeit der Souveränität beruhen, zu einer Anarchie in der internationalen Gemeinschaft in Bezug auf die Datengerichtsbarkeit geführt (Sun Nanxiang & Zhang Xiaojun 2015).

Die Zwangslage der nationalen Datensicherheit. Erstens sind Entwicklungsländer und am wenigsten entwickelte Länder im Vergleich zu Industrieländern offensichtlich weniger in der Lage, Daten zu kontrollieren. Obwohl sie über unabhängige Datenhoheit verfügen, sind alle Entwicklungsländer und weniger entwickelte Länder aufgrund des begrenzten Niveaus der Datentechnologie normalerweise nicht in der Lage, ihre eigene Datensicherheit und nationalen Interessen wirksam zu schützen. Zweitens ermöglicht die Revolution der Datentechnologie nicht nur einigen Industrieländern, die Datenhoheit zu missbrauchen, indem sie ihre technologischen Vorteile nutzen, sondern auch die Datensicherheit anderer Länder ernsthaft zu bedrohen. Nehmen wir die Vereinigten Staaten als Beispiel. Zusätzlich zu ihrer Kontrolle über extraterritoriale Daten durch Anwendung nationaler Gesetze sammeln und analysieren die Vereinigten Staaten mittels spezieller Projekte ihrer staatlichen Sicherheitsbehörden auch Daten, die der Zuständigkeit anderer Länder unterliegen. Schließlich macht es das spontane Spiel um die Datenhoheit auch

schwierig, die nationale Datensicherheit effektiv zu gewährleisten. Einerseits hat der grenzüberschreitende Datenfluss und die Datenspeicherung die effektive Zuständigkeit eines Landes für Daten und die zugehörigen Ausrüstungen erheblich abgeschwächt und eine ernsthafte Sicherheitslücke gebildet. Auf der anderen Seite können Industrieländer mit ihren fortschrittlichen Technologien Daten anderer Länder auf geheime Weise sammeln und überwachen, wodurch die Datenhoheit anderer Länder verletzt wird. Infolgedessen wird die Betonung der Unabhängigkeit der Datensouveränität zu Konfrontationen zwischen Ländern führen und einige Industrieländer dazu veranlassen, den Unilateralismus im Datenraum willkürlich umzusetzen.

Das spontane Spiel um Datenhoheit. Die Unabhängigkeit der Datensouveränität hängt eng mit dem Konflikt zwischen mehreren Zuständigkeiten und der Zwangslage in Bezug auf die nationale Datensicherheit zusammen, was zu einem spontanen Spiel führt, das den Zustand der Konfrontation über die Datenhoheit auslöst. Erstens wird die Betonung der absoluten Unabhängigkeit der Datenhoheit zu Konflikten zwischen mehreren Zuständigkeiten führen. Der Datenfluss bezieht sich mindestens auf Datenproduzenten, -empfänger und -nutzer, auf Orte der Übertragung, Transportation und des Bestimmungsorts, den Standort der Dateninfrastruktur, die Nationalität der Datendienstanbieter und den Ort des Datenbetriebs usw. Aufgrund der Unteilbarkeit und Integrität von Daten kann jeder Aspekt des grenzüberschreitenden Datenflusses zu Überschneidungen von Gerichtsbarkeiten und Konflikten um die Datenhoheit führen. Zweitens könnten die Länder zur Gewährleistung der Datensicherheit aufgrund der Unabhängigkeit der Datensouveränität die absolute einseitige Kontrolle über Daten und verwandte Technologien übernehmen. Insbesondere würden gesetzliche Beschränkungen für Wahl des Standorts von Rechenzentren auferlegt, die eine Einrichtung im Rahmen der vom Staat festgelegten Sicherheitskontrolle erfordern. Schließlich erhalten einige Industrieländer sensible Daten, indem sie die Datenhoheit anderer Länder aus dem Grund des Schutzes ihrer eigenen Datenhoheit verletzen. Zum Beispiel haben die Vereinigten Staaten ein Monopol über strategische Cyber-Ressourcen der Welt und eine große Anzahl von Top-Netzbetreibern und einflussreichsten Kommunikationsdienstleistern in der Welt, was es

ihnen ermöglicht, vertrauliche Daten aus anderen Ländern zu stehlen und eine Bedrohung zur globalen Datensicherheit darzustellen.

Vor dem Hintergrund der raschen Entwicklung und Popularisierung von Datentechnologien haben verschiedene Länder unterschiedliche Definitionen der Datenzuständigkeit aus unterschiedlichen Perspektiven vorgeschlagen. Insbesondere aufgrund der Unabhängigkeit der Datenhoheit beanspruchen viele Länder kontinuierlich das Zuständigkeitsrecht auf extraterritorialen Daten. Darüber hinaus ist die Kontrolle der Länder über ihre relevanten Daten im Zeitalter von Big Data stark geschwächt. Unter den Umständen von Konflikten um die Datenhoheit ist die Mehrheit der Entwicklungsländer und der am wenigsten entwickelten Länder nicht in der Lage, ihre eigene Datensicherheit zu gewährleisten und ihre Datenhoheit ohne Unterstützung eines wirksamen internationalen Koordinierungsmechanismus effektiv auszuüben. Im Gegenteil können Industrieländer dank fortschrittlicher Technologie Datenhoheit effektiv ausüben und sogar die Sicherheit und Datenhoheit anderer Länder gefährden. Unter diesem Gesichtspunkt führt die absolute Unabhängigkeit der Datensouveränität zu Konflikten mehrerer Gerichtsbarkeiten und Zwangslage in Bezug auf die nationale Datensicherheit, während das spontane Spiel und die Konfrontation schließlich Unordnung der internationalen Gesellschaft im Datenraum verursachen. Um die derzeitigen Störungen im Datenraum zu bekämpfen, soll man daher nach Wegen suchen, um entsprechende internationale Koordinierungsorganisationen oder -mechanismen einzurichten, die auf der Übertragbarkeit und Kooperativität der Datenhoheit beruhen (Sun Nanxiang & Zhang Xiaojun 2015).

(II) Übertragung der Datenhoheit

In der frühen Phase nach der Geburt der Souveränitätstheorie wurde allgemein angenommen, dass die Souveränität absolut, dauerhaft, unteilbar und nicht übertragbar sei. Wie ein amerikanischer Gelehrter in „Globalisierung und offene Gesellschaft“ betonte, „zerstört die Globalisierung souveräne Staaten, verbindet die Welt, missbraucht die von ihr gegründete politische Gemeinschaft, stellt den Gesellschaftsvertrag in Frage und

bringt die nutzlose Idee einer staatlich unterstützten sozialen Sicherheit lange vor der richtigen Zeit vor ... Von da an ist die Souveränität nicht mehr der unbestreitbare Grundwert wie früher“. Es ist mittlerweile veraltet, an der Absolutheit, Unteilbarkeit und Nichtübertragbarkeit der staatlichen Souveränität festzuhalten. Und die Zeit ist schon zu Ende, in der ein Land alle Angelegenheiten, die seine Souveränität betreffen, vollständig selbstständig regeln kann, ohne Kontrolle von außen und ohne den Eindruck andere Länder zu berücksichtigen, zu beeinflussen und Auswirkungen darauf zu haben. In der neuen Ära wird das Verhalten aller Länder zunehmend von verschiedenen anderen Akteuren beeinflusst und eingeschränkt. Angesichts dieser Realitäten der eingeschränkten Hoheit taucht die neue Idee, dass Souveränität übertragen werden kann, als neuer Trend auf. Im Allgemeinen glaubt man, dass sich die Übertragung der Souveränität auf einen Weg zur Ausübung der Souveränität bezieht, bei dem die souveränen Staaten im Kontext der Globalisierung und basierend auf der Aufteilung der Souveränität in identitätsbezogene und machtbezogene Elemente die staatlichen Interessen maximieren und eine positive Interaktion mit anderen Ländern und die internationale Zusammenarbeit fördern, ein Teil ihrer Souveränität an andere Länder oder internationale Organisationen gemäß dem Souveränitätsprinzip freiwillig übertragen, wobei das Recht vorbehalten bleibt, die Machtfunktionen der übertragenen Souveränität jederzeit zurückzuziehen.

„Der Souveränitätstransfer ist das Produkt der Kollision zwischen Globalisierung und staatlicher Souveränität. Es ist fundiert und unvermeidlich. Daher stehen die meisten Menschen dem Souveränitätstransfer positiv gegenüber“ (Yang Fei 2009). Das Konzept der „Souveränitätsübertragung“ ist jedoch seit seiner Entstehung umstritten. Der direkte Grund ist, dass Wissenschaftler dazu neigen, die staatliche Souveränität durch ihre verschiedenen Faktoren zu ersetzen, deren Hauptursache darin besteht, dass die staatliche Souveränität vielfältige Konnotationen beinhaltet. Die staatliche Souveränität enthält verschiedene Elemente wie die souveräne Identität, souveräne Autorität, souveräne Macht, souveränen Willen und souveräne Interessen usw. Dementsprechend ist die Antwort auf die Frage, ob diese Elemente übertragen werden können, unterschiedlich; einige Elemente wie souveräne Macht und souveräne Interessen usw. können übertragen werden,

während andere Elemente wie souveräner Wille, souveräne Autorität und souveräne Identität usw. nicht übertragbar sind. Derzeit gibt es noch keinen Konsens über den Begriff „Souveränitätsübertragung“, und Wissenschaftler verwenden manchmal unterschiedliche verworrene Formulierungen wie „Entfremdung der Souveränität“, „Abtretung der Souveränität“, „Negation der Souveränität“, „Aufgeben der Souveränität“ usw. (Yi Shanwu 2006).

Als Repräsentation, Erweiterung und Reflexion der nationalen Souveränität im Datenraum kann die Datenhoheit auch übertragen werden. Tatsächlich kann kein Land im Zeitalter von Big Data allein über den Datenraum verfügen, da Dateninfrastruktur und Datenaustauschzentren, die den Betrieb des Datenraums unterstützen, als „Globales Miteigentum“ betrachtet werden sollen. Die Offenheit des Datenraums erfordert natürlich, dass die Länder ihre nationalen Interessen innerhalb eines einheitlichen internationalen Rahmens wahren. Wenn die Datenhoheit verschiedener Länder vollständig verwirklicht werden sollen, muss ein Teil der Datenhoheit auf einen gemeinsamen Mechanismus oder eine gemeinsame Institution übertragen, damit sie diese Souveränität ausüben und das Miteigentum verwalten kann, nachdem sie diesen Teil der Souveränität erhalten hat. Als wichtige Manifestation der teilweisen Übertragung der nationalen Souveränität im Datenraum bedeutet die teilweise Übertragung der Datenhoheit nicht, die nationale Souveränität aufzugeben. Es ist vielmehr eine vernünftige Wahl nach seiner Einschätzung der Zeit und Umstände im Zeitalter von Big Data. Durch den Beitritt zu internationalen Organisationen und die Übertragung eines Teils ihrer Datenhoheit zur Ausübung durch eine kollektiv akzeptierte Organisation (Zhang Haibing 2005, S. 145) können Länder an die Datenhoheit teilhaben, langfristige nationale Interessen anstreben und die nationale Datenhoheit insgesamt schützen.

Die teilweise Übertragbarkeit der Datenhoheit besteht aus zwei Teilen, d.h. der teilweisen Übertragbarkeit der Datenzuständigkeit und der teilweisen Übertragbarkeit des Dateneigentums. Die Ersterer bedeutet, dass ein Land seine Datenzuständigkeit auf große Unternehmen übertragen kann, die sich an die Datenverwaltungsgesetze, -vorschriften und -richtlinien des Landes heilig halten, eine relativ unabhängige Zuständigkeit für Datenressourcen haben und damit verbundene Geschäftsaktivitäten im Rahmen der einschlägigen innerstaatlichen Gesetze und Vorschriften führen. Sie können

sogar ausländische multinationale Unternehmen sein, unterliegen jedoch der gesetzlichen Aufsicht und Kontrolle durch die zuständigen inländischen Behörden. Die teilweise Übertragbarkeit des Dateneigentums bedeutet, dass ein Land kein Eigentumsrecht auf Daten hat, die in seinem Hoheitsgebiet gespeichert oder berechnet, aber in anderen Ländern generiert werden. In diesem Fall soll das Eigentumsrecht auf diesen Daten, die in eigenem Hoheitsgebiet gespeichert oder berechnet sind, dem anderen Land übertragen werden. Der entscheidende Punkt für die teilweise Übertragbarkeit des Dateneigentums besteht darin, dass nicht alle in einem Land gespeicherten oder berechneten Daten Eigentum dieses Landes sein und von diesem verfügt werden können, da das Eigentumsrecht auf diesen Daten nur dem Land gehört, in dem diese Daten generiert worden sind, während andere Länder nur diejenigen Länder sind, in denen diese Daten zwar berechnet oder gespeichert werden, die aber kein Eigentumsrecht auf diese Daten haben.

Die Übertragung der Datenhoheit muss dem Grundsatz der Wahrung nationaler Interessen entsprechen. Wie der amerikanische Gelehrte Hans J. Morgenthau in „Dilemmas of Politics“ betonte, „kann die ultimative Sprache in der internationalen Politik tatsächlich nur nationale Interessen sein, solange die Welt politisch aus Ländern besteht“. Das zeigt, dass die nationalen Interessen die grundlegenden Ziele der Außenpolitik und des internationalen Verhaltens eines Landes bestimmen (Cai Gaoqiang 2002). Im Zeitalter von Big Data hängt es grundsätzlich von den nationalen Interessen ab, ob und wie ein Land Datenhoheit im Datenraum übertragen soll. Nur unter der Voraussetzung der Wahrung nationaler Interessen kann ein Land einen Teil seiner Datenhoheit übertragen. Die Übertragung der Datenhoheit „geht zum Teil zu Lasten vorübergehender und teilweiser Interessen im Austausch für die Förderung und Aufrechterhaltung langfristiger und gesamter Interessen“ (Li Huiying & Huang Guiqin 2004). Darüber hinaus ist die Übertragung der Datenhoheit durch ein Land weder uneingeschränkt und prinzipienlos, noch eine passive Aktion unter Druck einer Macht. In Bezug auf die Übertragung der Datenhoheit und die autonome Einschränkung soll auch das „Ausmaß“ sorgfältig abgewogen werden. D.h. dass die Unabhängigkeit und Selbstständigkeit der Länder sowie die Gleichberechtigung und den gleichen Status aller beteiligten Länder im Prozess der Übertragung der Datenhoheit gewährleistet werden müssen.

(III) Zusammenarbeit bei der Datenhoheit

Im Zeitalter von Big Data kann kein Land alle internationalen Angelegenheiten einseitig behandeln. Angesichts der Konflikte mehrerer Zuständigkeiten um Daten zwischen Ländern im Datenraum und der Notelage der nationalen Datensicherheit und der Probleme, die sich aus den besonderen Bedingungen der beteiligten Länder ergeben, sollen sich die Länder auf die Zusammenarbeit bei der Datenhoheit verlassen, um nach Lösungen zu suchen und die Spannungen zwischen den Ländern über die Datensouveränität an der Wurzel gründlich zu beseitigen, indem sie die Zuständigkeit angemessen definieren, das Miteigentum im Datenraum gemeinsam verwalten, kollektive Maßnahmen gegen Datenraumverbrechen und andere Kooperationsmodi ergreifen.

1. Souveränitätskooperation

In der internationalen Gemeinschaft hat jeder souveräne Staat die Freiheit und das Recht, rechtmäßig zu handeln. Mit anderen Worten, solange ein Staat nicht gegen verbietende Bestimmungen des Völkerrechts oder gegen die von ihm übernommenen bestimmten vertraglichen Verpflichtungen verstößt, kann er seine Souveränität frei ausüben, um seine eigenen Interessen zu verfolgen. In einer zunehmend vernetzten Welt reicht es jedoch nicht aus, immer komplexere und vielfältigere Probleme auf transnationaler Ebene zu lösen, wenn Staaten nur ihre Souveränität im Rahmen des rechtlichen Bereichs ausüben und frei handeln. Darüber hinaus werden die Einzelaktionen auf ihre eigene Weise und der freie Austausch zwischen Ländern auch zu gegenseitigen Verstößen führen (Zhao Zhou 2010, S. 153). Deshalb ist eine enge Zusammenarbeit mit der Souveränität erforderlich, und das letztendliche Ziel dieser Zusammenarbeit besteht darin, Interessen zu gewinnen. Souveränitätskooperation bedeutet „eine breite und umfassende Zusammenarbeit zwischen den Ländern, um „ihre jeweiligen Ziele auf der Grundlage einer vollständigen Anerkennung der Unterschiede zwischen ihren Zielen und der ‚Suche nach Gemeinsamkeiten unter Vorbehalt der Unterschiede‘ zu verwirklichen“ (Huang Houwen & Li Quanhui 2009). Außerdem muss die Zusammenarbeit

der Souveränität auf der Grundlage des Grundsatzes der Gleichheit der Souveränität, Einhaltung internationaler Gesetze, gutwilliger Erfüllung internationaler Verpflichtungen und ohne Einmischung in die inneren Angelegenheiten anderer Länder beruhen. Nur so kann man die gemeinsamen Interessen der Menschheit wahren“ (Ren Mingyan 2007).

Die besonderen Eigenschaften von Daten und Datenraum erfordern eine neue Art der Zusammenarbeit in der Souveränität. Mit der raschen Entwicklung und Verbreitung der Datentechnologie werden der grenzüberschreitende Fluss und die Speicherung von Daten immer häufiger und bequemer. Da Daten immateriell sind und global fließen, kann kein Land durch einseitige Bemühungen die absolute Kontrolle über Daten erlangen. Daher ist die Errichtung einer absoluten staatlichen Souveränität einfach ein „Wunschdenken“. Die Big Data ist von Natur aus international, und das damit verbundene Problem der Datenhoheit ist auch international. Kein Land kann internationale Angelegenheiten alleine behandeln. Angesichts der Probleme, die sich aus dem Konflikt zwischen mehreren Zuständigkeiten, der Notlage der Datensicherheit und den unterschiedlichen spezifischen Besonderheiten der Länder im Datenraum ergeben, sollen die Länder eine Zusammenarbeit in der Datensouveränität durchführen, um dieses Problem zu lösen. Die derzeitige Situation kann geändert werden, wenn die Länder ihre Zusammenarbeit im Bereich der Datenhoheit verstärken, damit sich der globale Datenfluss transparenter, besser reguliert und ordnungsmäßiger entwickeln kann. Eine solche Zusammenarbeit kann allen Ländern auch ermöglichen, die Daten der Partner wechselseitig wirksamer zu kontrollieren und angemessener zu nutzen, den Nutzungswert der Daten zu maximieren und die Spannungen über die Datensouveränität zwischen den Ländern vom Grund auf gründlich zu lösen.

2. Ideen der Zusammenarbeit bei der Datenhoheit

Die Länder haben das Recht, am Entscheidungsprozess für internationale Angelegenheiten Teilzunehmen, was eine wichtige Garantie für die Zusammenarbeit bei der Datenhoheit ist. Es ist nicht nur Sache der internationalen Gemeinschaft, sondern auch Verantwortung und Verpflichtung aller souveränen Staaten, zusammenzuarbeiten, um gemeinsame

Interessen, Sicherheit und Entwicklungsraum zu wahren. Gleichzeitig ist die Zusammenarbeit auch ein wichtiger Weg, um die Datenhoheit auszuüben. Im Zeitalter von Big Data soll sich jedes Land darüber im Klaren sein, dass andere Länder das Recht haben, die Datenressourcen, Datendienstleister und Dateninfrastrukturen in ihrem Hoheitsgebiet zu verwalten, und dass das einseitige Streben nach absoluter Unabhängigkeit der Souveränität zu Dilemma der Konfrontation zwischen Ländern führen kann. Um den grenzüberschreitenden Datenfluss und viele damit verbundene Probleme zu bewältigen, sollen wir auch auf die Frage zurückkommen, wie die Datenhoheit definiert werden soll. D.h., man soll Wert auf dem Recht auf Teilnahme an Entscheidungen in internationalen Angelegenheiten legen. Alle Länder der Welt, ob groß oder klein, reich oder arm, stark oder schwach, sind berechtigt, gleichberechtigt an der Entscheidung in internationalen Angelegenheiten teilzunehmen. Das ist die Grundlage der Zusammenarbeit im Bereich der Datenhoheit. Gleichzeitig ist es für jedes Land unmöglich, sich alleine mit internationalen Angelegenheiten zu befassen. Nur durch Zusammenarbeit in der Souveränität können wir gemeinsames Eigentum effektiv verwalten. Die Zusammenarbeit in der Souveränität ist der unvermeidliche Ansatz für Ausübung der Datenhoheit.

Die Zusammenarbeit im Bereich der Datenhoheit soll den Grundprinzipien des Völkerrechts, d.h. der Gleichheit der Souveränität, der Fairness und des gegenseitigen Nutzens entsprechen. Die souveräne Gleichheit aller Länder ist das Grundprinzip der „Charta der Vereinten Nationen“ und die Voraussetzung für Zusammenarbeit, während die Fairness aber der Kern einer neuen internationalen Ordnung ist. Einige Industrieländer implementieren aufgrund ihrer vorteilhaften Technologien eine unilaterale Kontrolle über Daten und damit verbundenen Einrichtungen, was die Interessen anderer Länder verletzt oder sogar opfert und somit zu Spannungen zwischen den Ländern hinsichtlich der Datensicherheit führt. Daher ist es für die Zusammenarbeit bei der Datenhoheit von entscheidender Bedeutung, einen machtorientierten Ansatz im Datenraum zu vermeiden. Der letztendliche Grund für Zusammenarbeit ist die wirksame Verwaltung, Kontrolle und Nutzung des gemeinsamen Datenraums. Diese Zusammenarbeit soll im Einklang mit den Grundsätzen der Gleichheit,

des beidseitigen Gewinns und des gegenseitigen Nutzens erfolgen, anstatt eigene nationale Interessen auf Kosten der Interessen anderer Länder zu erfüllen. Um Fairness zu erreichen, soll die internationale Gemeinschaft Entwicklungsländern, insbesondere den am wenigsten entwickelten Ländern, Unterstützung in Bezug auf Datentechnologie bieten, um ihre Fähigkeit zu steigern, ihre eigenen Daten zu verwalten, zu kontrollieren und zu verwenden und Bedrohungen der Datensicherheit wie Datenhegemonie und Datenterrorismus von außen zu verhindern.

3. Modell der Zusammenarbeit bei der Datenhoheit

Die Abwägung und Regulierung der Ausübung der Zuständigkeit ist der Hauptinhalt der Zusammenarbeit im Bereich der Datenhoheit, deren Kernidee darin besteht, den Umfang der Zuständigkeit angemessen zu definieren. Diese Definition muss auf der Basis der Souveränität und der Regierungsmacht sowie auf einer angemessenen Abgrenzung des Grundsatzes der hoheitsgebietsbezogenen Zuständigkeit und personenbezogenen Zuständigkeit beruhen. Aus Sicht des traditionellen Völkerrechts wird ein Staat als unteilbares und einheitliches Ganzes betrachtet, der für alle Einzelpersonen innerhalb des Hoheitsgebiets oder zumindest für ihre Handlungen verantwortlich ist. Dementsprechend wird der Zuständigkeitsrahmen der geltenden Gesetze sowie die Rechte und Pflichten ihrer relevanten Subjekte anhand des Standorts von Dingen oder Personen bestimmt. Datenhoheit und Regierungsmacht sind eng miteinander verbunden. Es ist für kein Land möglich, die Zuständigkeit für Personen oder Dinge auszuüben, die außerhalb seiner Kontrolle liegen. Aufgrund der Besonderheiten der Daten können Probleme der Grenzlosigkeit des Datenraums mit traditionellen Zuständigkeitsgrundsätzen jedoch nicht gelöst werden. Daher sollen die Länder auf der Grundlage des Kerngeistes der traditionellen Gerichtsbarkeitstheorie das am engsten verwandte Prinzip der Wirkungsgerichtsbarkeit als Mithilfe aufnehmen. Wenn sich ein Land bei Ausübung der Datengerichtsbarkeit auf Personen und Standorte anderer Länder erstreckt oder erhebliche Auswirkungen auf die Staatssicherheit, soziale Ordnung und wirtschaftlichen Interessen anderer Länder hat, haben die betroffenen Länder das Recht,

die Datenzuständigkeit auszuüben und dieses Land aufzufordern, seine übermäßig ausgeweitete Zuständigkeitsmacht einzuschränken.

Als das wichtigste Gebiet der Datenspeicherung und des Datentransports wird der Datenraum als „Global öffentliches Gebiet“ angesehen oder auch als „globales Miteigentum“ bezeichnet, das ähnliche Merkmale wie Hohe See, Polarregionen, internationaler Luftraum und Weltraum etc. aufweist. Im Zeitalter von Big Data kann kein Land den Datenraum allein in Besitz nehmen. Das bedeutet, dass Daten und zugehörige Einrichtungen, die den Betrieb des Datenraums unterstützen, als „globales Gemeineigentum“ betrachtet werden sollen. Da der Datenraum offen ist, sollen alle Länder natürlich ihre nationalen Interessen im gesamten Rahmen der Vereinten Nationen wahren. Um die Datenhoheit jedes Landes vollständig zu verwirklichen, müssen wir daher bei der Datenhoheit zusammenarbeiten, indem gemeinsame Verwaltungsbehörden oder -mechanismen kooperative Souveränität genießen und ausüben und den gemeinschaftlichen Gegenstand verwalten. Aktuelle Konflikte sind dem Wesen nach darauf zurückzuführen, dass einige Industrieländer die unilaterale Zuständigkeit für den Datenraum verfolgen, um die staatlichen Sicherheit und Entwicklungsinteressen für sich selbst zu suchen. Der Datenraum ist Teil des Gemeineigentums der Menschheit. Daher sollen Daten und die dazugehörigen Einrichtungen, die die Entwicklung und den Betrieb des Datenraums unterstützen, in gewissem Maße nicht zu einem bestimmten Land gehören, sondern über eine Art internationales Kondominium kontrolliert werden.

Da der Datenraum immateriell, virtuell und grenzenlos ist und das Niveau der Datentechnologie in den meisten Entwicklungsländern, insbesondere in den am wenigsten entwickelten Ländern begrenzt ist, sodass sie Verbrechen im Datenraum, insbesondere Datenterrorismus durch wirksame Ausübung der Gerichtsbarkeit der Daten innerhalb oder außerhalb ihres Hoheitsgebiets nicht effektiv bewältigen können. Ein wirksamer Weg zur Lösung dieses Problems der Datensicherheit besteht darin, einen Sicherheitsmechanismus zu verfolgen, der eine kollektive Zusammenarbeit in der internationalen Gemeinschaft auf der Grundlage der Datensouveränität beinhaltet. Obwohl der Mechanismus der internationalen Zusammenarbeit zur Bekämpfung der Kriminalität im Datenraum immer ausgereifter geworden ist, ist die Rechtsverbindlichkeit des von der internationalen

Gemeinschaft formulierten einschlägigen Verhaltenskodex derzeit noch relativ schwach. Daher ist es dringend erforderlich, Maßnahmen für Verbesserung und Institutionalisierung kollektiver Aktivitäten zur Bekämpfung krimineller Handlungen im Datenraum zu ergreifen. Kriminelle Aktivitäten im Datenraum beziehen sich auf Interessen und Sicherheit aller Länder, und die meisten wichtigen kriminellen Aktivitäten sind eng mit dem Datenterrorismus verbunden, der das Überleben, die Sicherheit und Entwicklung der gesamten Menschheit unmittelbar bedroht. Im Hinblick darauf ist es nicht nur wichtig, sondern auch notwendig, einen kollektiven Sicherheitsmechanismus für den Datenraum einzurichten. Die Vorgehensweise, einigen Industrieländern bei der Festlegung und Durchsetzung von Regeln freie Hand zu lassen, widerspricht der Idee der Zusammenarbeit bei der Datenhoheit. Die Zusammenarbeit unter der Voraussetzung der Übertragung der Datenhoheit erfordert die Festlegung eines vollständigen Verhaltenskodex für den Datenraum innerhalb eines einheitlichen internationalen Rahmens. Angesichts des schweren Daten-Terrorismus können sogar transnationale Maßnahmen auf der Grundlage des Rechts auf kollektive Selbstverteidigung in Betracht gezogen werden.

Abschnitt IV Verwaltung der Datensouveränität

Die Wahrung der Datenhoheit ist für die Sicherheit und Entwicklung des Staates von großer Bedeutung, steht in der Praxis aber vor schweren Herausforderungen. Der Datenhegemonismus, Datenprotektionismus, Datenkapitalismus und Datenterrorismus etc. hat Auftrieb bekommen. Ohne Regulierung müsste ein Chaos im globalen Datenraum herrschen. Daher ist es dringend erforderlich, ein Regulierungssystem für Datensouveränität auf der Grundlage des Grundsatzes der Datenhoheit aufzubauen. In Übereinstimmung mit der aktuellen internationalen politischen Landschaft bietet die Verwaltung der Datensouveränität einen institutionalisierten und realistischen Weg zur Regulierung des Cyberspace. Da die Datenhoheit eines der Kernkonzepte des chinesischen Datenrechtssystems ist, müssen wir die Konnotation der Datensouveränität aus der Sicht

des gesetzlichen Regulierungssystems herausuchen und ihre Eptaxie klarstellen, um ein System aufzubauen und letztendlich die Datenhoheit im Rahmen der Rechtsstaatlichkeit umzusetzen.

(I) Globaler Trend der Datenhoheit

Gegenwärtig ist die Datenhoheit nicht nur zu einem neuen Wettbewerbsfeld zwischen Ländern der Welt geworden, und einige Probleme in diesem Bereich haben, sondern auch sogar neue Engpässe und Risiken für das globale Wirtschaftswachstum und die soziale Entwicklung mit sich gebracht. Daher ist die Verwaltung der Datensouveränität mehr und mehr zu einem zentralen Thema aller Länder der Welt geworden. Der Datenraum hat die grundlegenden Merkmale des anarchischen Zustands. In gewissem Sinne ist der derzeitige Datenraum ein anarchisches öffentliches Globalgebiet wie Hohe See und der Weltraum. Unter diesem internationalen anarchischen Umstand steht die Verwaltung der Datensouveränität gerade vor einer Reihe neuer Herausforderungen wie Datenhegemonismus, Datenprotektionismus, Datenkapitalismus und Datenterrorismus usw.

1. Datenhegemonismus

Mit dem Zusatzantrieb des Zeitalters von Big Data hat sich die traditionelle Hegemonie neu entwickelt. Einige große Länder haben begonnen, neben der traditionellen militärischen, politischen und wirtschaftlichen Hegemonie auch die Datenhegemonie zu verfolgen und den Datenhegemonismus umzusetzen. Sie nutzen die Abhängigkeit der Menschen von Daten und die Verwundbarkeit der Datengesellschaft, übernehmen die Kontrolle über Daten als Mittel, um den Zweck der Manipulation oder Kontrolle der Welt zu verwirklichen. Theoretisch steht der Datenhegemonismus der Datensouveränität gegenüber. Das Prinzip der Datenhoheit ist, dass alle Länder in den internationalen Beziehungen gleiche Rechte haben. In der Praxis stellt der Datenhegemonismus jedoch eine „ernsthafte Bedrohung für die Souveränität und die staatliche Sicherheit

aller Länder sowie für den Weltfrieden dar. Einige mächtige Länder überschreiten nicht nur bestimmte Grenzen bei der Ausübung ihrer Macht, sondern erweitern ihre Macht auch auf die Souveränität anderer Länder“ (Schlüssel-Labor für Big Data Strategie 2019, S. 272–273). Das Vorhandensein von Datenhegemonismus ist derzeit die größte Bedrohung für die Verwaltung der Datensouveränität, da er die Bemühungen schwächerer Länder im Datenraum behindert, inländische Big Data effektiv zu verwalten, und die Verwirklichung einer wirksameren Verwaltung der Datensouveränität verhindert.

2. Datenprotektionismus

Der grenzüberschreitende Datenfluss hat zu einem Wachstum der globalen digitalen Wirtschaft geführt und ist im Zeitalter von Big Data der wertvollste Handelskanal geworden. Die Länder legen jedoch weiterhin unterschiedliche Beschränkungen für den grenzüberschreitenden Datenfluss fest. Insbesondere nach dem „Snowden-Vorfall“ haben mehrere Länder den grenzüberschreitenden Datenfluss durch strenge Verwaltungsanforderungen auf Datenlokalisierung eingeschränkt oder verboten. Die Richtlinien zur Datenlokalisierung bieten in den meisten Ländern eine Rechtsgrundlage für die Sicherheit des Staates und den Schutz der Privatsphäre der Bürger. Gleichzeitig haben einige Länder begonnen, extreme Datenlokalisierungsmaßnahmen zu ergreifen, um den grenzüberschreitenden Datenfluss völlig einzuschränken oder zu verbieten, um bestimmte wirtschaftliche Ziele zu erreichen. Die extreme Praxis der Datenlokalisierung hat Bedrohungen aufgrund von Überwachung, d.h. Datenprotektionismus, mit sich gebracht. International ist der Datenprotektionismus nicht nur mit dem raschen Fluss von Daten, Kapital, Technologie und Personal in der Weltwirtschaft unvereinbar, sondern widerspricht auch der Strategie der Datensouveränität, die von der Mehrheit der Länder der Welt befürwortet wird, und hat keinen Respekt vor der Datenhoheit anderer Länder. Der Datenprotektionismus kann die Risiken des grenzüberschreitenden Datenflusses nicht wirksam verhindern. Stattdessen wird er wahrscheinlich den Wettbewerb und die Reibung zwischen den Ländern verschärfen und zu extremem Egoismus

und Unilateralismus führen, digitalen Handelskrieg und Datenkonfrontation auslösen und die Welt im Zeitalter von Big Data in eine ernstere und weitverbreitete Krise versenken.

3. Datenkapitalismus

Daten bedeuten nicht nur, Informationen einfach aufzuzeichnen und zu speichern. Sie sind sondern auch ein Schatz von großem kommerziellem Wert. Im Allgemeinen sind Daten eine Art wertvoller unbekannter „Nachrichten“. Man erhält Daten, weil er ihren Nutzungswert bevorzugt. Ein unvermeidliches Ergebnis der Entwicklung des Kapitalismus ist, dass Daten zu Kapital werden. Das Datenkapital ist eine neue Form von Kapital, das nach Geldkapital und Wissenskapital entsteht. Es ist eine Kombination aus Monopolkapital der Datentechnologieindustrie und Finanzmonopolkapital. Dem Wesen nach ist es Datenmonopol. Das Datenmonopol beschleunigt den Kapitalzuwachs auf ein beispielloses Niveau und bildet so den Datenkapitalismus. Als eine Form des Kapitalismus hat der Datenkapitalismus „eine Art Kapitalmonopol geschaffen, das wir seit der Einführung des Kapitalmonopols nie gesehen haben, und diese Form des Monopols wird unter dem Deckmantel des ‚geistigen Eigentums‘ in zunehmendem Maße verschlimmert“ (Yan Xianjun 2001). Der Datenkapitalismus kann den grundlegenden Widerspruch des Kapitalismus, der im Zeitalter von Big Data noch komplizierter wird, nicht vollständig auflösen. Einerseits kontrolliert und manipuliert der Datenkapitalismus die Datenproduktion und -verbreitung im Datenraum, indem er seine modernsten Datentechnologien nutzt, um in die Datensouveränität anderer Länder einzufallen und Gewinne daraus zu erzielen. Andererseits strebt der Datenkapitalismus mit Kontrolle über Datentechnologie nach politischen, wirtschaftlichen, kulturellen und anderen Interessen, vergrößert die globale Datenlücke und löst die globale Krise der Datensicherheit aus. Daher kann der Datenkapitalismus das tief verwurzelte Problem der Verwaltung der Datensouveränität weder wissenschaftlich und effektiv lösen noch die Absicht haben, neue Herausforderungen zu bewältigen, die sich aus der unausgewogenen Entwicklung ergeben. Im Gegenteil ist

der Datenkapitalismus zu einem wichtigen Problem geworden, das im Prozess der Verwaltung der Datensouveränität dringendst gelöst werden muss.

4. Datenterrorismus

Im Zeitalter von Big Data ist der traditionelle Terrorismus nicht nur nicht verschwunden. Ganz im Gegenteil hat er mithilfe von Big Data sondern auch eine sprunghafte Entwicklung realisiert, sodass die terroristischen Aktivitäten vom physischen Raum zum Datenraum erweitert werden können. Die Big Data bietet Terroristen neue Mittel und Plattformen. Terroristen nutzen Big Data nicht nur als Waffen, um Zerstörung durchzuführen und Beunruhigung anzustiften, sondern auch mit den Big Data dazu, Terroristen zu rekrutieren, Spenden zu sammeln sowie terroristische Aktivitäten zu planen und umzusetzen. Mit der Entwicklung und breiten Anwendung von Big Data verkörpern sich die global zunehmenden terroristischen Bedrohungen allmählich in den Datenterrorismus, dessen Lebenskraft, Beeinflussungsfähigkeit und Zerstörungskraft viel größer als die des traditionellen Terrorismus sind (Schlüssel-Labor für Big Data Strategie: 2019, S. 279). Der Datenterrorismus hat alle Gemeinsamkeiten mit dem traditionellen Terrorismus, hat jedoch eine ernstere Asymmetrie und ist stärker getarnt als der traditionelle Terrorismus. Im Vergleich mit dem traditionellen Terrorismus schadet der Datenterrorismus der nationalen Souveränität, dem Weltfrieden und der Sicherheit der internationalen Gemeinschaft noch schwerer, indem er mit Hilfe von Big Data terroristische Aktivitäten durchführt, was auch noch verheerendere Folgen hat. Der Datenterrorismus ist nicht nur eine neue Methode des Terrorismus, sondern auch „ein neues globales Problem im Bereich der nichttraditionellen Sicherheit“ (Yu Xiaoqi 2002). Gegenwärtig stellt der Datenterrorismus eine ernsthafte Bedrohung für die wirtschaftliche Entwicklung, die soziale Sicherheit und die Stabilität in bestimmten Ländern und sogar der Welt dar und hat die Verwaltung der Datensouveränität vor großen Herausforderungen gestellt. Alles in allem hat er sich als ein dringendes Problem für alle Länder der Welt herausgestellt, deren Lösung auch dringendst notwendig ist.

(II) Internationale Divergenz bei der Datensouveränität

Der Cyberspace ist zweifellos ein wichtiges Feld für Ausübung der Datenhoheit. Da das „Verständnis des Cyberspace, die praktischen Erfahrungen in verschiedenen Ländern sehr begrenzt sind und der Unterschied und sogar der Antagonismus in Bezug auf Ideologie, Wertanschauung und realistische nationale Interessen sehr groß ist“ (Huang Zhixiong & Ying Yaohui 2017), hat die internationale Gesellschaft derzeit in vielen Bereichen des Cyberraums immer noch viele Meinungsverschiedenheiten. Zusammenfassend gibt es Divergenz in Bezug auf Verständnis, Strategie und Verwaltung.

1. Kognitive Divergenz: Globales Gemeingebiet vs. souveränes Hoheitsgebiet

Gegenwärtig gibt es in der internationalen Gemeinschaft zwei sehr unterschiedliche Auffassungen zum Attribut des Cyberraums. Einige glauben, dass es sich um „Globales Gemeingebiet“ handelt, während andere es als „souveränes Hoheitsgebiet“ betrachten. Die Ersteren umfassen die Vereinigten Staaten, Japan, die Europäische Union sowie einige weitere Länder und Organisationen, die im Cyberspace hoch entwickelt sind. Sie glauben, dass der Cyberspace, der sich vom physischen Raum unterscheidet, keiner Gerichtsbarkeit und Herrschaft eines einzigen Landes unterliegt und als globales Gemeingebiet wie die Hohe See und der Weltraum angesehen werden sollte. Das „globale Gemeingebiet“ bezieht sich auf „Ressourcen oder Gebiete, die von keinem Land dominiert werden, von denen die Sicherheit und der Wohlstand aller Länder abhängen“. Die Vereinigten Staaten stellen beispielsweise den Cyberspace mit den Ozeanen, dem internationalen Luftraum und dem Weltraum auf eine Stufe und klassifizieren den Cyberspace als „globales Gemeingebiet“, das außerhalb der Reichweite eines einzelnen souveränen Staates liegt. „Im Jahr 2005 haben die USA den Cyberspace in der ‚Strategie für innere Sicherheit und zivile Unterstützung‘ als Globales Gemeingebiet eingestuft und den Cyberspace im ‚Quadriennale Defense Review 2010‘ als globale Domäne innerhalb des Informationsumfelds definiert“ (Huang

Zhixiong 2017, S. 98–99). Die Vereinigten Staaten sind der Ansicht, dass der Cyberspace zum „globalen Gemeingebiet“ gehört und dass sein Management die Grenzen zwischen den souveränen Staaten im traditionellen Sinne überschreiten sollte. Das heißt, Länder dürfen keine Souveränität im Cyberspace ausüben. In scharfem Gegensatz dazu sind andere Befürworter der Theorie des „souveränen Hoheitsgebiets“, die hauptsächlich von Russland, Brasilien, der Shanghai Kooperationsorganisation (SCO), dem Rat für Sicherheitskooperation im asiatisch-pazifischen Raum (CSCAP) und anderen Schwellenländern und Organisationen im Cyberspace vertreten werden, der Ansicht, dass der Cyberspace seine eindeutige Eigenschaft der Souveränität hat. Um die soziale Stabilität aufrechtzuerhalten, sollen Länder ihre Souveränität im Cyberraum errichten und ausüben. Beispielsweise haben Russland mit China und anderen SCO-Mitgliedstaaten 2011 auf der 66. Tagung der Generalversammlung der Vereinten Nationen den „Internationalen Verhaltenskodex für Informationssicherheit“ vorgelegt und vorgeschlagen, dass das Entscheidungsrecht auf politische Autorität für öffentliche Fragen im Zusammenhang mit dem Internet Teil der staatlichen Souveränität ist, weshalb die Souveränität jedes Landes im Cyberspace respektiert werden soll. Das CSCAP ist auch der Ansicht, dass der Cyberspace keineswegs das sogenannte „globale Gemeingebiet“ ist. Stattdessen ist er ein wichtiger Bestandteil der nationalen Souveränität und ein neuer Hoheitsbereich für Entwicklung verschiedener Länder. Dieser neue Bereich bezieht sich auch auf realistische Themen wie die Aufrechterhaltung der nationalen Souveränität, der Sicherheit und Entwicklungsinteressen. Obwohl viele Länder heute befürworten, dass man im Cyberspace nationale Souveränität ausüben soll, gibt es derzeit aufgrund der erheblichen Unterschiede in Bezug auf Entwicklungsstand, Geschichte, Kultur und Sozialsystem offensichtliche Verschiedenheiten (Liu Ying & Wu Ling 2019) in Bezug darauf, wie sie die Eigenschaft des Cyberspace wirklich verstehen und damit umgehen. Infolgedessen besteht eine große Lücke in Bezug auf die Frage der Cyberspace-Souveränität bei den einschlägigen internationalen Bemühungen zur Festlegung von Regeln. Dementsprechend wird die „Daten-Souveränität“ als untergeordneter Begriff der Cyberspace-Souveränität auch in der heutigen internationalen Gemeinschaft auf sehr

unterschiedliche Weise verstanden. Es gibt sogar Meinungsverschiedenheiten und Konflikte derart, ob die Datenhoheit gerechtfertigt werden kann oder ob sie auch in der Cyberspace-Souveränität enthalten ist.

2. Divergenz in der Strategie: Cyber-Liberalismus gegen Schicksalsgemeinschaft im Cyberspace

Unter Berücksichtigung der Wertanschauung befürworten die westlichen Länder einstimmig die Idee, dass die „Menschenrechte der Souveränität überlegen“ sind. Sie befürworten die Heiligkeit und Unverletzlichkeit der grundlegenden Menschenrechte der Bürger. In ähnlicher Weise halten sie im Cyberraum am Cyberliberalismus fest und lehnen die Ausweitung der Kontrolle vom physischen Raum auf den Cyberspace ab. Sie glauben, dass die staatlichen Datengrenzen die Demokratie vor Herausforderungen stellten und brachten zum Ausdruck, keine Maßnahmen, die den freien Datenfluss behindern könnten zu akzeptieren. Zum Beispiel sind die Vereinigten Staaten der Meinung, dass die freie Verbindung und der freie Datenfluss aus keinem Grund von einem Staat behindert werden dürften und die grundlegende Freiheit im Cyberspace garantiert werden sollte. Deshalb haben die Vereinigten Staaten 2011 die „Internationale Strategie für den Cyberspace“ und die „Handlungsstrategie für den Cyberspace“ nacheinander herausgegeben, um die Freiheit im Cyberspace zu fördern. Diese beiden Dokumente bilden den Gesamtrahmen des internationalen Internet-Strategiesystems der Vereinigten Staaten, dessen Grundlage die Theorie des Liberalismus im Cyberspace ist. Mit der Freiheit im Cyberspace als Kernkonzept und wichtige Komponente behauptete „die internationale Strategie für den Cyberspace“, dass die „internationale Strategie für den Cyberspace“ die Grundprinzipien der Vereinigten Staaten widerspiegelt, d.h. die Kernzusage zu Grundfreiheit, Privatsphäre und freiem Datenfluss“. „Nach ihrer Entstehung wurde die Theorie des Cyber-Liberalismus zur offiziellen Ideologie der US-Regierung und gilt als unbestreitbarer universeller Wert. Mithilfe der starken Ausbreitungskraft des von den USA geführten westlichen Diskurssystems hat diese Theorie in den letzten Jahren die Forschung und Diskussion im Zusammenhang mit dem Cyberspace praktisch dominiert“ (Li Chuanjun 2019). Im Gegensatz

zu Behauptungen der Cyberliberalisten sind die Entwicklungsländer im Cyberspace der Ansicht, dass „der Cyber-Liberalismus den Bedürfnissen im Cyberspace widerspricht“ (Wang Mingjin 2016). Im Bereich des Cyberspace soll man den Grundsätzen der internationalen Beziehungen und der „Charta der Vereinten Nationen“ folgen, die territoriale Integrität, politische Unabhängigkeit und die Freiheit der Menschenrechte aller Länder respektieren und den Grundsatz der Übereinstimmung der staatlichen Sicherheit mit der souveränen Unabhängigkeit einhalten. Kein Land darf Cyber-Hegemonie unter dem Banner der „Cyber-Freiheit“ betreiben. Als Beispiel misst China der Cyber-Souveränität große Bedeutung bei und setzt sich in den letzten Jahren als eine seiner zentralen Aussagen in Bezug auf das Völkerrecht und die internationale Ordnung im Cyberspace für die Achtung und Wahrung der Cyber-Souveränität aller Länder ein. Im Dezember 2015 stellte der chinesische Staatspräsident Xi Jinping auf der 2. Weltinternetkonferenz zuerst das Konzept des „Aufbaus einer Schicksalsgemeinschaft im Cyberspace“ vor und legte „vier Prinzipien“ und „fünf Wege“ zur Verwirklichung der Schicksalsgemeinschaft im Cyberspace tief gehend dar. Dieses Konzept entspricht den Interessen der meisten Länder und wurde bald darauf von immer mehr Ländern akzeptiert. Trotzdem haben einige westliche Länder jedoch aufgrund ideologischer Überlegungen und anderer Faktoren immer noch bestimmte Bedenken.

3. Verwaltungsdivergenz: mehrinteressenseitige Verwaltung vs. multilaterale Verwaltung

Gegenwärtig bilden Länder im Hinblick auf das Modell der Cyberspace-Verwaltung hauptsächlich zwei Gruppierungen: Eine sind Industrieländer im Cyberspace, die von den Vereinigten Staaten angeführt werden, und die andere sind Schwellen- und Entwicklungsländer im Cyberspace, die von China, Russland und Brasilien vertreten werden. Das erstere Lager befürwortet das Modell der mehrinteressenseitigen Verwaltung, während die Letztere die multilaterale Verwaltung unterstützt. Der „mehrinteressenseitige Ansatz“, der derzeit ein „allgemein anerkanntes“ Verwaltungsmodell im globalen Cyberspace ist, befürwortet eine

„Verwaltung des Cyberspace, die von „technischen Experten, Handelsinstitutionen und der Zivilkörperschaften dominiert wird, während Regierungen und sogar zwischenstaatliche Organisationen wie die Vereinten Nationen auch nicht darin eingreifen sollten“ (Wang Mingjin 2016). Dieses Modell unterstreicht die Beteiligung mehrerer Verwaltungsgremien, legt mehr Aufmerksamkeit auf Verweigerung der nationalen Souveränität und Betonung der Einzelnen und „glaubt, dass die globale und dezentrale Cyberspace-Übertragung die Regierungen ihrer zentralen Leitungsposition in der traditionellen Regierungsführung schon beraubt hat“ (Zheng Wenming 2017) und befürwortet den Ansatz „von unten nach oben“ in der Cyberspace-Regulierung. Das mehrinteressenseitige Regulierungsmodell scheint eine bestimmte Rolle bei der Abwägung der Interessen aller Parteien zu spielen, aber aufgrund des Mangels an Zusammenarbeit und Unterstützung durch souveräne Staaten ist es unwahrscheinlich, dass eine wirksame Verwaltung des Cyberspace mit diesem Modell erreicht werden kann. Darüber hinaus weist dieses mehrinteressenseitige Regulierungsmodell auch eine Reihe von Mängeln auf und sieht sich im Cyberspace weitverbreiteten Zweifeln von Schwellen- und Entwicklungsländern hinsichtlich seiner Angemessenheit, Legitimität und Zuverlässigkeit gegenüber. Im Vergleich dazu unterstützt das zweite Lager von breiten Schwellen- und Entwicklungsländern im Cyberspace tendenziell die von Regierungen dominierte multilaterale Verwaltung und befürwortet die Verstärkung der Cyberspace-Verwaltung im Rahmen der Vereinten Nationen oder anderer internationaler Organisationen. Dieser Vorschlag wird als „Multilaterales Regulierungsmodell“ bezeichnet. Dieses Modell befürwortet ein „von oben nach unten“-Modell für die Cyberspace-Verwaltung durch staatliche Funktionsstellen. Es betont „das Prinzip der nationalen Souveränität im Cyberspace und strebt eine Lösung der Frage der Unordnung im Cyberspace an, wobei die Nationalstaaten die zentrale Rolle spielen. Ein Staat soll die Macht haben, die digitale Souveränität und staatliche Sicherheit im Cyberspace zu schützen; und im Rahmen der Vereinten Nationen soll eine Art reelle Organisation eingerichtet werden, deren Hauptakteure Staaten sind, die die Fragen im Zusammenhang mit der Cyberspace-Verwaltung koordiniert und behandelt“ (Zheng Wenming 2017). Daraus ist ersichtlich, dass Konflikte zwischen diesen beiden

Modellen kontinuierlich auftreten. „Die Unterschiede zwischen beiden Lagern sind im Wesentlichen Streitigkeiten zwischen Konservativen und Reformern in Bezug auf den Cyberspace-Verwaltungs-Mechanismus, die jeweils auf ihren eigenen Interessen behaupten. Es kann vorausgesagt werden, dass die Verschiedenheiten und das Spiel um dieses Thema noch lange bestehen werden“ (Long Kun & Zhu Qichao 2019).

(III) Gesetzliche Regelung der Datensouveränität

Die Wahrung der Datenhoheit ist von großer realistischer Bedeutung für die Sicherheit, wirtschaftliche Entwicklung und soziale Stabilität des Staates. In der Praxis steht die Datensouveränität jedoch vor vielen neuen Bedrohungen und Herausforderungen. Daher ist es dringend erforderlich, ein System aufzubauen und einen Weg der Gesetzgebung zur Wahrung der Datensouveränität zu erkunden, um relevante Anstrengungen auf den Weg der gesetzesbasierten Regulierung zu bringen. Dies wird dazu beitragen, das Risiko eines Missbrauchs der Datenhoheit zu verringern und eine gesunde Entwicklung in diesem Bereich zu fördern.

1. Herausforderungen der Datenhoheit

Gegenwärtig haben immer mehr Länder Praktiken in Bezug auf die Gesetzgebung zur Datensouveränität durchgeführt. Die internationale Gemeinschaft hat aber noch keinen Konsens über die in diesem Aspekt zu befolgenden Grundsätze der Datensouveränität erzielt. Einerseits vertreten Russland, die Europäische Union und die Vereinigten Staaten aufgrund ihrer unterschiedlichen nationalen Interessen verschiedene Ansichten zur Ausübung der Datenhoheit. Russland setzt sich aktiv für die Ausübung der Datensouveränität aus Gründen der Staatssicherheit ein. Die EU und ihre Mitgliedstaaten respektieren auch die Datensouveränität zum Schutz der personenbezogenen Daten der Bürger, während die Vereinigten Staaten und einige andere Länder achten aber stärker auf die kommerziellen Vorteile durch Big Data und befürworten einen freien grenzüberschreitenden Datenfluss. Andererseits hat die

Datensouveränität für Länder, die unterschiedliche Kontrollfähigkeit für Daten haben, auch unterschiedliche Bedeutung. Im Vergleich dazu neigen Länder mit schwacher Kontrollfähigkeit im Cyberspace dazu, das Konzept der Datensouveränität zu akzeptieren, um ihre Rechte auf Datenverwaltung und -nutzung durch internationale Zusammenarbeit stärker zu schützen. Im Gegenteil machen sich Länder mit starker Kontrollfähigkeit über Daten keine Sorgen darüber, dass ihre Daten geplündert oder ausgebeutet werden, und für sie ist es wirklich von weniger Bedeutung, ob die Datenhoheit betont werden soll oder nicht (He Bo 2017). Gleichzeitig steht die Datenhoheit als ein neues Recht der Staaten vor vielen neuen Herausforderungen und Bedrohungen, darunter dem Datenhegemonismus, Datenprotektionismus, Datenkapitalismus und Datenterrorismus. Viele westliche Länder, angeführt von den Vereinigten Staaten, haben relativ vollständige und ausgereifte Rechtssysteme für das Datenmanagement eingerichtet, die gesamten Industrieketten auf der Grundlage ihrer technologischen Vorteile gebildet, die von inländischen Branchenriesen erbracht wurden, und die wichtigsten Punkte des Datenmanagements beherrscht und tatsächlich anderen Ländern Datenhegemonie auferlegt. Mit dem PRISM-Überwachungsprogramm beispielsweise erlaubte die US-Regierung ihrer Nationalen Sicherheitsagentur den direkten Zugriff auf die riesigen Datenressourcen von neun großen Unternehmen, darunter Google, Facebook, Microsoft, YouTube und PalTalk, um die benötigten Informationen und Nachrichten zu erhalten, die schwerwiegende Verstöße gegen die Datensicherheit und nationalen Interessen anderer Länder verursachten (Du Yanyun 2016).

2. Aufbau eines Systems für Datenhoheit

Gegenwärtig konzentrieren sich Gesetze und Richtlinien in Bezug auf die Datenhoheit hauptsächlich auf die Verwaltung und Kontrolle von Daten. Die Ansprüche und Praktiken verschiedener Länder in Bezug auf die Datenhoheit konzentrieren sich hauptsächlich auf die Verwaltung des grenzüberschreitenden Datenflusses. International haben immer mehr Länder und Regionen begonnen, ihre gesetzliche Datenhoheitssysteme zum Zweck des Datenmanagements aufzubauen (He Bo 2017).

Beim Aufbau des Rechtssystems für die Datenhoheit soll man nicht nur auf Sicherheit und Schutz der Kerndaten aus Sicht der Risikoprävention achten, sondern auch mehr Wert auf den Abbau und die Nutzung von Big-Data-Ressourcen legen und noch vorsichtiger vor technologischen Risiken und wirtschaftlichen Verlusten durch Datenhegemonie sein. Daher sollen wir beim Festlegen relevanter Regeln und beim Aufbau der Systeme an drei Dimensionen arbeiten: transnationaler Datenfluss basierend auf Datenklassifizierung, lokalisierte Speicherung von Datenressourcen und Beseitigung der Datenhegemonie durch Aufbau einer Schicksalsgemeinschaft (Zhang Jianwen & Jia Zhangfan 2018).

Datenkontrolle und Datenfluss basierend auf Klassifizierung. Im Zeitalter von Big Data entspricht es den grundlegenden und langfristigen Interessen der meisten Länder, einen freien Datenfluss unter der Voraussetzung der Wahrung der staatlichen Sicherheit zu realisieren. Dies erfordert, dass alle Länder Daten auf der Grundlage der Klassifizierung verwalten, um das Auslaufen kritischer Daten zu verhindern, den ordnungsgemäßen und freien Fluss unkritischer Daten in Übereinstimmung mit dem Gesetz zu gewährleisten und ein Regelwerk für grenzüberschreitenden Datenfluss zu bilden, das sowohl Sicherheit als auch Freiheit gebührend berücksichtigt. Um Datenlecks zu vermeiden, sollen wir Modelle für die dynamische Verfolgung des Datenflusses und die Bewertung des Sicherheitsrisikos erstellen, einen pluralistischen Mechanismus für retrospektive Rechenschaftspflicht und einen Notfallreaktionsmechanismus für Sicherheitsrisiken einrichten. Diese drei „zusammengebildeten“ universellen Mechanismen für pluralistische retrospektive Rechenschaftspflicht, Risikoeinschätzung und dynamische Verfolgung helfen uns, das Auslaufen kritischer Daten zu verhindern und die durch Datenauslauf verursachten Verluste des Staates mit dem Notfallreaktionsmechanismus zu minimieren. Um den Fluss unkritischer Daten zu fördern, sollen wir das Konzept der Bescheidenheit und Zurückhaltung sowie das Subsidiaritätsprinzip einführen und den freien Austausch und Fluss unkritischer Daten unterstützen, um beiden Seiten des Spiels Vorteile auf der Grundlage der ausreichenden Entfaltung der jeweiligen besonderen Fähigkeiten und der einander ergänzenden Vorteile zu verschaffen.

Lokalisierte Speicherung von Daten und Schutz der Schlüsselinfrastruktur. Bei der Datenlokalisierung liegt der Schwerpunkt auf den

lokalisierten Daten, wobei all diese (Datenerfassung, -verarbeitung und -speicherung usw.) im Zuständigkeitsbereich des betreffenden Landes durchgeführt werden müssen. Beim Aufbau eines Datenhoheitssystems müssen wir jedoch die Replizierbarkeit und Mobilität von Daten berücksichtigen, um den umgekehrten Einschränkungseffekt und regulatorischen Auslauftreffekt durch überlagerte Datenhoheitszuständigkeiten zu vermeiden. Neben der lokalisierten Speicherung von Daten sollen alle Länder auch detaillierte Regeln festlegen, wo sich Schlüsselinfrastrukturen wie Betreiber und Serviceeinrichtungen etc. befinden sollen. Insbesondere sollen Betreiber juristische Personen oder nichtjuristische Personen sein, die im Hoheitsgebiet eines Landes registriert sind; und für den Standort der Server sollen auch klare Vorschriften für Genehmigung vor der Einrichtung und / oder Überprüfung nach der Einrichtung erstellt werden. Darüber hinaus sollen der Infrastruktur angemessene Vertraulichkeits- und Sicherheitsstufen zugewiesen werden, um die Schlüsselinfrastruktur besser vor Hackerangriffen zu schützen.

Beseitigung der Datenhegemonie und Aufbau einer Schicksalsgemeinschaft. Um die Datenhegemonie zu beseitigen, sollen die Entwicklungsländer einerseits das strategische Design auf höchster Ebene stärken und einheimischen Big-Data-Unternehmen mehr Unterstützung bieten, um das Monopol der Hegemonialmächte auf Datentechnologien zu brechen; und andererseits sollen sie auch daran arbeiten, eine Schicksalsgemeinschaft aufzubauen, um die Basis der Legitimität der Datenhegemonie zu untergraben. Obwohl die Datenhoheit Daten umfasst, die von Bürgern eines Landes in anderen Ländern generiert worden sind, ist es zweifellos notwendig, die Unterstützung und Mitwirkung anderer Länder sicherzustellen, um die Datenhoheit wirklich auszuüben. Zu diesem Zweck müssen wir den „regulatorischen Auslauftreffekt“ vermeiden, die zu institutionellem Gegenangriff durch „umgekehrte Beschränkungen“ aus anderen Ländern führen können. Andernfalls würde es schwierig sein, den freien Datenfluss zu realisieren und eine extraterritoriale Zuständigkeit zu etablieren. Durch Stärkung der multilateralen Zusammenarbeitsmechanismen können wir die Bildung neuer Regeln für den grenzüberschreitenden Datenfluss fördern und ein brandneues System für grenzüberschreitenden Datenfluss auf der Grundlage von Gleichheit und gegenseitigem Nutzen aufbauen. Dies

wird die durch den Datenhegemonismus hervorgerufene Ungleichheit der Entwicklungschancen wirksam zersetzen sowie Weisheit und Aufschluss über Bildung neuer internationaler Beziehungen geben.

3. Vorschlag für Gesetzgebung zur Datensouveränität

Die amerikanische Wissenschaftlerin Lisa J. Damon wies am Ende des 20. Jahrhunderts darauf hin, dass der grenzüberschreitende Datenfluss theoretisch Völker der ganzen Welt näher bringen, die Distanz in der physischen Welt verringern, Daten sofort verfügbar machen und zu einer voneinander abhängigen globalen Wirtschaft beitragen soll. In der Realität schafft der grenzüberschreitende Datenfluss jedoch neue Hindernisse zwischen verschiedenen Ländern. Um weiteren Schaden zu vermeiden, müssen wir neue Vereinbarungen treffen und wirksame internationale Entscheidungsgremien einrichten (Zhu Gaofeng 2016). „Bei der Formulierung von Gesetzen zur Datensouveränität sollen wir einen mehrdimensionalen und ganzheitlichen Ansatz verfolgen und verschiedene relevante Aspekte umfassend berücksichtigen, da die Sicherheit der nationalen Datenhoheit ein pluralistisches, multilaterales, demokratisches und integriertes System ist, an dem mehrere Parteien beteiligt haben“ (Qi Aimin & Zhu Gaofeng 2016).

Auf Ebene der inländischen Gesetze. Gegenwärtig gibt es in einigen Gesetzen und Vorschriften Chinas Bestimmungen zum Schutz der Datensouveränität, aber keine eindeutigen Gesetze oder Vorschriften sind diesem Thema zum Schutz der nationalen Datensouveränität gewidmet. Eine vorläufige klassifizierte Statistik gemäß der „Zusammenstellung von Gesetzen und Vorschriften zur chinesischen Internetbranche“ (2018) zeigt, dass der Schutz der Datensicherheit im Cyberspace in China derzeit vor allem noch am Schutz der Netzwerkinfrastruktur, Datensysteme und Datenschwachstellen verbleibt und dass sich keine Gesetze oder Vorschriften speziell auf die nationale Datenhoheit konzentrieren. Daher ist derzeit dringend notwendig, Vorschriften für die Datensicherheit im Netzwerk und Cyberspace und für Wahrung der nationalen Datensouveränität zu erlassen. Zu diesem Zweck soll China auf nationaler Ebene die Gesetze und Vorschriften in Bezug auf die Datenhoheit aktiv verbessern, schneller vorgehen, um den

rechtlichen Status der Datenhoheit festzustellen, hart daran arbeiten, einen spezifischen Rahmen für die Gesetzgebung zur Datenhoheit zu schaffen und die Datenhoheit im Rahmen der Gesetze auszuüben, um Datensicherheit und nationale Interessen zu schützen. Auf der internationalen Ebene soll China die Erfahrungen und Methoden, die es aus der Zusammenarbeit mit anderen Ländern in verschiedenen Bereichen gewonnen hat, in vollem Umfang nutzen und von westlichen Ländern und Gebieten lernen und ihre fortgeschrittenen Erfahrungen für den Datenschutz als Beispiel nehmen. Dies wird uns trotz des Mangels an solider Gesetzgebung zur Datenhoheit ermöglichen, aufgrund der tatsächlichen nationalen Verhältnisse einen systematischen Rechtsrahmen für Datenrechte aufzubauen, unseren Datenüberprüfungsmechanismus zu vervollständigen und unsere technologische Fähigkeit zur datenbezogenen Gesetzgebung gemäß unseren spezifischen Bedingungen zu erhöhen.

Auf Ebene der internationalen Gesetze. Die Datenhoheit zeigt klare Merkmale eines internationalen Problems. Im Zeitalter von Big Data sind alle Länder in Bezug auf Verletzung ihrer Datenhoheit Bedrohungen ausgesetzt, und kein Land kann sich vollständig davon fernhalten. Daher sollen sich die Länder im Prinzip der „Suchen nach Gemeinsamkeiten unter Zurückstellung von Differenzen“ aktiv an der Formulierung internationaler Vorschriften zur Datensicherheit und der Abschließung einschlägiger Verträge über Datensicherheit beteiligen. Diese Abkommen sollen verschiedene Formen annehmen, sodass sie umfassend berücksichtigt sind, eine vollständige Abdeckung haben und den „ganzheitlichen Sicherheitsansatz“ widerspiegeln. Der Abschluss solcher Verträge über Datensicherheit soll auch vielfältig erfolgen, sie können sowohl regionale als auch bilaterale und sogar multilaterale Verträge sein. Die Datenhoheit ist untrennbar mit der nationalen Souveränität verbunden, wobei die nationale Souveränität die Datenhoheit umfasst. Daher sollen die Grundprinzipien der nationalen Souveränität auch für die zu schließenden Datensicherheitsverträge gelten, während Ziele und Zwecke sowie konkrete Inhalte und die Verpflichtungen und Verantwortlichkeiten jeder Vertragspartei in diesen abzuschließenden Datensicherheitsverträgen klar festgelegt sollen. Insbesondere sollen diese Verträge hauptsächlich darauf abzielen, die internationale Gemeinschaft in Richtung zur Realisierung der Datensicherheit zu lenken, Länder und

Regionen zu leiten, um die internationale Zusammenarbeit zu stärken, den Missbrauch von Daten und die Verletzung und Schädigung der Datensouveränität verschiedener Länder zu bekämpfen und nicht sicherheitsrelevante Risiken, die die politische, wirtschaftliche und soziale Datensicherheit usw. anderer Länder bedrohen, zu beseitigen und eine faire und gerechte Verteilung der Datenressourcen und Aufrechterhaltung eines sicheren, stabilen und freien Datenbetriebs zu gewährleisten (Qi Aimin & Zhu Gaofeng 2016).

Literaturverzeichnis

- Aristoteles: „Politik“, übersetzt von Wu Shoupeng: Die kommerzielle Presse, 1996.
- Cai Cuihong: „Das Konzept von Datensouveränität und seine Anwendungsperspektive in der Cloud-Ära“, in *Zeitgenössische Internationale Beziehungen*, 12/2013.
- Cai Gaoqiang: „Über die Übertragung von Souveränitätsmacht in der Globalisierung“, in *Journal der Hunan Political-Legal Cadre College*, 5/2002.
- „Caroline-Affäre: Wie soll ein Staat sein Selbstverteidigungsrecht ausüben?“, http://www.sohu.com/a/300675149_120094707. 12. 03. 2019.
- Chen Xujing: „Neueste Theorien der Souveränität“, übersetzt von Zhang Shibao, Tsinghua University Press, 2010.
- Du Yanyun: „Nationale Datensouveränität in der Big-Data-Ära“, in *International Review*, 3/2016.
- Du Zhichao u. Nan Yuxia: „Untersuchungen zum Verhältnis zwischen Netzwerksouveränität und nationaler Souveränität“, in „*Journal der Südwesten Petroleum Universität*“ (Edition Sozialwissenschaften), 6/2014.
- Fang Binxing, Zou Peng u. Zhu Shibing: „Forschung zur Cyberspace-Souveränität“, in *Strategische Studie zu CAE*, 6/2016.
- Fang Binxing: „Zur Cyberspace-Souveränität“, Wissenschaftspresse, 2017.
- Fang Binxing: „Diskussion über das auf Nationsunion basierende autonome Root-Nameserver aufgrund der nationalen Cyber-Souveränität“, in „*Informationssicherheit und Kommunikationsgeheimhaltung*“, 12/2014.
- Gu Dexin: „Konflikte in den Gesetzen des Krieges“, in „*Internationales Forum*“, 1/2001.

- He Bo: „Studie über Rechtspraktiken und vorgeschlagene Gegenmaßnahmen zur Datensouveränität“, in Informationssicherheit und Kommunikationsgeheimhaltung, 5/2017.
- He Fuyong u. Duan Jindong: „Völkerrechtliche Perspektive des nationalen Selbstverteidigungsrechts im Antiterrorismus“, in „Forum der Weltwirtschaft und -politik“, 2/2005.
- Huang Houwen u. Li Quanhui: „Zusammenarbeit ist der Grundstein der nachhaltigen Entwicklung und der harmonischen Gesellschaft“, in „Heutiges Südchina“, „Theoretische Innovation“, 12/2009.
- Huang Zhixiong u. Ying Yaohui: „Einfluss der USA auf das Völkerrecht im Cyberspace und ihr Aufschluss für China“, in „Fudan Kommentar zu internationalen Beziehungen“, 2/2017.
- Huang Zhixiong: „Über Cyber-Souveränität: Rechtstheorie, Politik und Praxis“, Sozialwissenschaftliche akademische Presse, 2017.
- Jean-Jacques Rousseaus: „Gesellschaftsvertragstheorie“, übersetzt von Yang Guozheng, Volksverlag Shaanxi, 2006.
- Jennings & Watts: „Oppenheimer Völkerrecht“, übersetzt von Wang Tiewa et.al. Verlag der Chinesischen Enzyklopädie, 1995.
- Jiang Ruihao: „Kurze Analyse der Cyber-Souveränität“, Legality Vision, 2016, 13. Ausgabe.
- Li Aijun u. Zhang Jun: „Die rechtliche Natur und Eigenschaften des Datenrechts. Vortrag auf dem Summit for Big Data im Rahmen der Rechtsstaatlichkeit in Peking – Beitragssammlung zu Big Data, neue Wachstumspunkt, neue Triebkraft und neue Ordnung“, 2017.
- Li Chuanjun: „Ordnungsänderung und Modellkonstruktion von Global Governance im Cyberspace“, in Zeitschrift der Wuhan Universität für Wissenschaft und Technologie (Social Science Edition), 1/2019.
- Li Huiying u. Huang Guiqin: „Über die Übertragung der staatlichen Souveränität“, in Hebei Rechtswissenschaft, 7/2004.
- Liu Qingjian: „Analyse der Theorie der staatlichen Souveränität“, in „Journal der Chinesischen Renmin Universität“, 6/2004.
- Liu Ying u. Wu Ling: „Globale Verwaltung im Cyberspace: Chaos, Chancen und Chinas Vorschläge“, in Erkenntnis und Praxis, 1/2019.
- Long Kun u. Zhu Qichao: „Regelsetzung für den Cyberspace: Konsens und Zwietracht“, in Global Review, 3/2019.
- Qi Aimin u. Zhu Gaofeng: „Zur Einrichtung und Verbesserung des nationalen Datenhoheitssystems“, in Journal Suzhou Universität (Auflage Philosophie und Sozialwissenschaften), 1/2016.
- Qi Juxun: „Gerichtsbarkeitsfrage im Internet“, in „Lanzhou Academic Journal“, 5/2003.

- Ren Mingyan: „Eine Studie zur staatlichen Informationssouveränität vor dem Internet- Hintergrund“, in Hebei Rechtswissenschaft, 6/2007.
- Schlüssellabor für Big Data-Strategie: „Blockdaten 5.0: Theorie und Methode der Datensoziologie“, CITIC Verlag, 2019.
- Shi Yuhang: „Cybergrenze der Souveränität - aus Blickwinkel der Regulierung von grenzüberschreitender Datenübertragung“, in „Informationszeitschrift“, 9/2018.
- Sun Nanxiang u. Zhang Xiaojun: „Zur Datensicherheit: Eine Untersuchung von Spiel und Zusammenarbeit im Cyberspace“, in Pazifik Journal, 2/2015.
- Wang Mingjin: „Die Zukunft der globalen Cyberspace-Verwaltung: Souveränität, Wettbewerb und Konsens“, in Volksforum, an akademischer Front, 4/2016.
- Wang Xiangrong: „Kurzer Überblick auf die Gleichberechtigungsrecht in der Verfassung unseres Landes“, in „Rechtsstaatlichkeit und Gesellschaft“, 18/2019.
- Wang Yuan, Huang Daoli u. Yang Songru: „Studie über die Natur und das Eigentum an Datenrechten“, in Informationssicherheit und Kommunikationsschutz, 5/ 2017.
- Wu Shan & Liu Yading: „Integrationsprozess der Hoheit und Gleichberechtigung“, in „Die heutige Welt und der Sozialismus“, 1/2010.
- Xiao Dongmei u. Wen Yuheng: „Verteidigung der nationalen Datensouveränität in der globalen Datenflut“, in Manuskript mit roter Flagge, 9/2017.
- Xie Yongjiang: „Studie über Prinzipien des Cybersicherheitsrechts“, Jinan Journal (Philosophie & Sozialwissenschaft Edition), 6/2018.
- Yan Xianjun: „Informationskapitalismus ist eine neue Stufe in der Entwicklung des Kapitalismus“, in „Entdeckung“, 6/2001.
- Yang Fei: „Versuchsweise Analyse der Definition des Begriffs der Übertragung der staatlichen Souveränität“, in „Journal der Hochschule für internationale Beziehungen“, 2/2009.
- Yang Xiaotong: „Hobbes's Theorie der bösen Natur und Vertragsstaat“, in „Literarische Bildung“, 32/2018.
- Yi Shanwu: „Eine neue Sicht auf die Übertragung von Staatssouveränität“, in „Journal der Chongqing Verkehrsuniversität“ (Edition Sozialwissenschaften), 3/ 2006.
- Yu Xiaoqi: „Trends und Merkmale der globalen Cyberinformationssicherheit“, in „Zeitgenössische Internationale Beziehungen“, 2/2002.
- Yu Zhigang: „Einhaltung der Cyber-Souveränität und der Daten-Souveränität und Aufbau eines internationalen Internet-Verwaltungssystems“, in Prokurator-Tageszeitung, 13. Dezember 2016.
- Zhang Haibing: „Forschung über europäisches Integrationssystem“, Shanghai Academy of Social Sciences Press, 2005.

- Zhang Jianwen u. Jia Zhangfan: „Interpretationslogik und Systemkonstruktion der Datensouveränität aus rechtlicher und wirtschaftlicher Sicht“, in Journal Chongqing Universität für Post und Telekommunikation (Sozialwissenschaft Edition), 6/2018.
- Zhang Jingwen: „Forschung über völkerrechtlichen Vorschriften für Datenhoheit“, Doktorarbeit, Universität der inneren Mongolei, 2018.
- Zhang Naigen: „Forschung über zeitgenössisches Völkerrecht“, Volksverlag Shanghai, 2002.
- Zhao Gang, Wang Shuai u. Wang Peng: „Forschung über technologisches Konzept der Big-Data-Verwaltung in Bezug auf Datenhoheit“, in „Cyberraumsicherheit“, 2/2017.
- Zhao Zhou: „Über souveräne Verantwortung“, Rechtsverlag, 2010.
- Zheng Wenming: „Chinas Wahl im Internet-Verwaltungsmodell“, in Chinesische Sozialwissenschaften, 17. August 2017.
- Zhou Gengsheng: „Internationales Recht (I)“, Die kommerzielle Presse. 1981.
- Zhu Gaofeng: „Die Etablierungs- und Gesetzgebungsvorschläge der nationalen Informationssouveränität in der Big-Data-Ära“, 7/2016.
- Zhu Qi: „Über Ordnungsansicht in den Souveränitätsgedanken von Jean Bodins“, in „Sozialwissenschaft Guizhou“, 12/2015.
- Zhu Yanxin: „Frage der Netzwerk-Souveränität aus der Perspektive des Völkerrechts“, Journal des Politologischen Instituts Xi'an, 2017.

Datenrechtssystem: Ein internationaler Vergleich

Das Datenrecht ist ein gemeinsames wichtiges Thema der ganzen Welt und sein Schutz ist eine wichtige Strategie der Gesetzgebung aller Länder. Die Vereinigten Staaten betrachten den Schutz von Datenrechten als eines der Objekte der Rechte auf Privatsphäre im weiteren Sinne. Die Europäische Union argumentiert die Notwendigkeit des Schutzes von Datenrechten aus Sicht der Persönlichkeitsrechte, während Japan die Vorteile des anglo-amerikanischen Rechtssystems und des Kontinentalrechtssystems besser kombiniert. Basierend auf dem Konzept einer Schicksalsgemeinschaft der Menschheit und Aufbau einer solchen Gemeinschaft im Cyberspace befürwortet China, dass „alle Länder der Welt die Zusammenarbeit stärken, den Austausch vertiefen, die Möglichkeiten einer digitalisierten, internetbasierten und intelligenten Entwicklung gemeinsam gut nutzen und auf die Herausforderungen bei der Entwicklung der Big-Data-Branche in Bezug auf Aspekte wie Recht, Sicherheit und Regierungsverwaltung usw. gut zu bewältigen“. Auf der Grundlage der Zusammenfassung der neuesten technologischen Fortschritte, Trends und Modi der Gesetzgebung zu Datenrechten im Ausland und in Ausrichtung des Aufbaus einer internationalen Rechtsgemeinschaft haben wir relevante Untersuchungen durchgeführt, um einen Fahrplan für die Gesetzgebung zu Datenrechten vorzulegen und darauf hinzuweisen, dass das Datenrechtsgesetz eine großartige Vorstellung ist, um zu verstehen, wie das Leben in Zukunft aussehen wird. Das ist eine wichtige Entdeckung in der Erforschung der digitalen Zivilisation und ein wichtiges juristisches Instrument für unsere Teilnahme an der globalen Verwaltung.

Abschnitt I Datenrechtssysteme des Auslandes

Die Gesetzgebung zu Datenrechten ist eine nationale Strategie im Zeitalter von Big Data und eine wichtige Aktivität, um das Rederecht auf der internationalen Bühne für die Gesetzgebung zu Datenrechten zu bekommen. Die Gesetzgebung zum Schutz personenbezogener Daten in den 1970er-Jahren markierte den Beginn einer „Blütezeit“ in der Gesetzgebung zum Schutz von Datenrechten im Ausland. Alle Länder der ganzen Welt haben Pläne gemacht und strategische Schritte in Richtung einer Gesetzgebung im Zusammenhang mit Datenrechten unternommen. Entsprechend den verfügbaren Statistiken haben mehr als 110 Länder oder Regionen Gesetze zum Schutz von Datenrechten erlassen. Hier konzentrieren wir uns auf Sortierung und Vergleich der Praktiken und Untersuchungen ausländischer Datenrechtssysteme in Bezug auf Recht, Sicherheit und Regierungsverwaltung usw., um einige Regelmäßigkeiten, Muster und Erfahrungen aus ihren Praktiken zur Gesetzgebung zu Datenrechten herauszufinden.

(I) Vergleich des gesetzlichen Schutzes von Datenrechten

Der Schutz personenbezogener Daten stellt eine neue Herausforderung für die globale Verwaltung von Daten dar und ist zu einem Schwerpunkt der Gesetzgebung in verschiedenen Ländern geworden (siehe Tabelle 5-1). Offensichtlich ist Europa bei der Gesetzgebung zum Schutz personenbezogener Daten weltweit führend, da die meisten europäischen Länder bereits Gesetze zum Schutz personenbezogener Daten erlassen und relevante Systeme verbessert haben. Einige Länder wie die Schweiz und Deutschland usw. haben beispielsweise bereits in den 1970er-Jahren Gesetze zum Schutz personenbezogener Daten erlassen. Was die amerikanischen Länder betrifft, so haben die Vereinigten Staaten in den 1970er-Jahren die Führung bei der Einführung von Datenschutzgesetzen übernommen und den Anwendungsbereich dieses Schutzrechts auf Kinder ausgedehnt. Die ozeanischen Länder haben gegen Ende des vorigen

Jahrhunderts Gesetze zum Schutz personenbezogener Daten erlassen. Die überwiegende Mehrheit der afrikanischen Länder hat bis auf wenige Ausnahmen wie Südafrika und Tunesien bisher kein Datenrechtssystem eingerichtet. Israel ist das erste der neun asiatischen Länder, die Gesetze zum Schutz personenbezogener Daten erlassen haben, während Japan über die detailliertesten Gesetze zum Schutz personenbezogener Daten mit sorgfältiger und verfeinerter Kategorisierung verfügt.

In den ausländischen Gesetzgebungspraktiken zu Datenschutzrechten gibt es hauptsächlich drei grundlegende gesetzliche Konzepte für Datenrechte, nämlich „personenbezogene Daten“, „personenbezogene Informationen“ und „Privatsphäre“. Solche Länder, Regionen und Organisationen, die die „Personenbezogenen Daten“ als grundlegenden Begriff des Datenrechts benutzen, sind am meisten, vor allem sind sie wie der Europäische Rat, die Europäische Union und ihre Mitgliedstaaten sowie viele andere Länder, die sich stark an der „EU-Richtlinie zum Schutz personenbezogener Daten“ (1995) orientiert haben. „In Ländern des Gemeinrechts wie den USA, Australien, Neuseeland, Kanada sowie vielen APEC-Mitgliedstaaten, die stark von den USA beeinflusst sind, ist der Begriff der ‚Privatsphäre‘ populärer verwendet, während in Japan, Südkorea, Russland und anderen Ländern der Begriff „persönliche Informationen“ bevorzugt wird“ (Zhou Hanhua 2005). Darüber hinaus werden auch andere Grundkonzepte wie das „persönliche Leben“ (z. B. im chilenischen Gesetz zum Schutz des persönlichen Lebens) sowie „persönliche Daten und Privatsphäre“ (z. B. in den OECD-Richtlinien zum Schutz der Privatsphäre und zum grenzüberschreitenden Fluss personenbezogener Daten) verwendet. „Konzeptionelle Unterschiede beruhen hauptsächlich auf unterschiedlichen Rechtstraditionen und Verwendungspraktiken, haben jedoch keinen Einfluss auf die Konnotation der Rechtskonzepte in ihrer wesentlichen Bedeutung“ (Zhou Hanhua 2005).

In Bezug auf Inhalte der Gesetzgebung zum Datenrecht im Ausland haben die Gesetze zum Schutz privater Daten in verschiedenen Ländern, Regionen und internationalen Organisationen drei gemeinsame Eigenschaften: Erstens ist das Objekt des rechtlichen Schutzes die Einzelperson als natürliche Person und nicht Unternehmen, Regierung oder andere Organisationen, auch keine Roboter oder „Gen-editierten Menschen“. Zweitens

übernimmt der rechtliche Schutz personenbezogener Daten die Grundsätze der Rechtmäßigkeit, Legitimität, Notwendigkeit, des begrenzten Zwecks und der Datenminimierung, um die maximalen legitimen Rechte und Interessen der Datenrechtsinhaber zu schützen. Drittens besteht das Ziel der Gesetze darin, Verletzung der persönlichen Datenrechte zu verhindern, indem verhindert wird, dass identifizierbare personenbezogene Daten nach Belieben gesammelt, gespeichert, übertragen und illegal verwendet werden. Deshalb liegt der Schwerpunkt der Gesetzgebung zum Schutz personenbezogener Daten nicht auf „personenbezogenen Daten“ selbst, sondern auf den „Verhaltensweisen oder Aktivitäten im Zusammenhang mit der Verarbeitung personenbezogener Daten“. Aus diesen Gründen heben viele Länder, Regionen oder Organisationen den Begriff der „Verarbeitung“ in ihren Rechtsvorschriften besonders hervor. Beispiele hierfür sind der Europäische Rat, die Europäische Union, San Marino, Island, Griechenland und Dänemark usw.

Tabelle 5-1 Datenrechtsgesetzsysteme in wichtigen Ländern und Regionen

Kontinent	Land/Region	Jahr	Bezeichnung des Rechts
Europa	Schweden	1973	Datengesetz
		1998	Gesetz über personenbezogene Daten
	Finnland	1999	Gesetz über personenbezogene Daten
	Dänemark	1978	Gesetz über private Datenbank
		1987	Gesetz über Behördendatenbank
		2000	Gesetz zur Verarbeitung personenbezogener Daten
	Norwegen	1978	Gesetz über die Registrierung privater Daten
		1978	Gesetz über öffentliche Datenbank
		2000	Gesetz über personenbezogene Daten
	Frankreich	1978	Datenschutzgesetz
		2016	Gesetz der digitalen Republik
	Österreich	1978	Datenschutzgesetz (geändert 2012)
	Deutschland	1977	Bundesdatenschutzgesetz (geändert 1980, 1990, 2001, 2003, 2005, 2006, 2009, 2015, 2017)

Tabelle 5-1 Fortsetzung

Kontinent	Land/Region	Jahr	Bezeichnung des Rechts
Europa	Belgien	1992	Datenschutzgesetz (geändert 1998)
	Luxemburg	1979	Gesetz über beschränkte Nutzung von elektronischen Computern verarbeiteten Daten
		2002	Gesetz zum Schutz von Privatsphäre bei der Verarbeitung personenbezogener Daten
		2005	Besondere Bestimmungen zum Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation
	Schweiz	1992	Bundesgesetz über den Datenschutz
	Spanien	1992	Gesetz zur Regulierung der automatisch behandelten personenbezogenen Daten (geändert 1999)
		1999	Gesetz zum Schutz der automatisch verarbeiteten personenbezogenen Daten
	Portugal	1991	Gesetz zum Schutz personenbezogener Daten während der automatischen Verarbeitung
		1998	Gesetz zum Schutz personenbezogener Daten
	Italien	1996	Datenschutzgesetz
	Griechenland	1997	Gesetz zum Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten
	Vereinigtes Königreich	1984	Datenschutzgesetz
		1998	Datenschutzgesetz
	Irland	1988	Datenschutzgesetz
		2003	Datenschutzgesetz (Änderung)
	Russland	2015	Gesetz zum Schutz personenbezogener Daten
	Rumänien	2001	Gesetz zum Schutz der Privatsphäre in Bezug auf die Verarbeitung und den freien Verkehr personenbezogener Daten

(Fortsetzung)

Tabelle 5-1 Fortsetzung

Kontinent	Land/Region	Jahr	Bezeichnung des Rechts
Amerika	Vereinigte Staaten	1970	Fair Credit Reporting Act
		1974	Datenschutzgesetz (staatlich)
		2000	Gesetz zum Schutz der Online-Privatsphäre von Kindern
		2014	Datenschutz und Smart Grid: Ein freiwilliger Verhaltenskodex
		2015	Verbraucher-Privatsphäre-Schutzgesetz
	Kanada	1983	Privatsphäre-Schutzgesetz
		2000	Gesetz zum Schutz personenbezogener Daten und elektronischer Dokumente
		2003	Gesetz zum Schutz personenbezogener Daten
	Argentinien	1998	Gesetz zum Schutz personenbezogener Daten
		2000	Gesetz zum Schutz personenbezogener Daten
	Chile	1999	Gesetz zum Schutz des Privatlebens
	Uruguay	2002	Datenschutzgesetz
	Brasilien	1997	Datenschutzgesetz
	Paraguay	2000	Gesetz zum Schutz personenbezogener Daten
	Bahamas	2003	Datenschutzgesetz (Privatsphäre personenbezogener Informationen)
Asien	Südkorea	1997	Gesetz zum Schutz personenbezogener Daten an öffentlichen Stellen
		2011	Gesetz zum Schutz personenbezogener Informationen
	Japan	1988	Gesetz zum Schutz personenbezogener Daten im Zusammenhang mit der elektronischen Datenverarbeitung durch Verwaltungsorgane
		1989	Gesetz zum Schutz personenbezogener Daten im Zusammenhang mit der elektronischen Datenverarbeitung durch nicht öffentliche Dienststellen

Tabelle 5-1 Fortsetzung

Kontinent	Land/Region	Jahr	Bezeichnung des Rechts
		2003	Gesetz zum Schutz personenbezogener Informationen im Besitz selbständiger Verwaltungsbehörden usw.
		2003	Gesetz zur Offenlegung von Informationen und zum Schutz personenbezogener Daten
		2003	Gesetz zum Schutz personenbezogener Daten
	Singapur	2002	Gesetz zum Schutz von Informationen in privaten Institutionen
		2012	Gesetz zum Schutz personenbezogener Daten
	Israel	1981	Schutz der Privatsphäre (geändert 1985)
	Thailand	1997	Offizielles Informationsgesetz
	Armenien	2002	Gesetz der Republik Armenien zum Schutz personenbezogener Daten
	Vereinigte Arabische Emirate	2007	Datenschutzgesetz
	China	2016	Cyber-Sicherheitsgesetz
	Sonderverwaltungszone Hongkong	1995	Verordnung über personenbezogene Daten (Privatsphäre)
	Sonderverwaltungszone Macao	1995	Gesetz zum Schutz personenbezogener Computerdaten
		1996	Durchführungsbestimmungen für das Gesetz zum Schutz computerverarbeiteter personenbezogener Daten
		2005	Gesetz zum Schutz personenbezogener Daten (Privatsphäre-Schutzgesetz)
	Taiwan, China	1995	Gesetz zum Schutz computerverarbeiteter personenbezogener Daten
		1996	Durchführungsbestimmungen für das Gesetz zum Schutz computerverarbeiteter personenbezogener Daten

(Fortsetzung)

Tabelle 5-1 Fortsetzung

Kontinent	Land/Region	Jahr	Bezeichnung des Rechts
Ozeanien	Australien	1988	Privatsphäre-Schutzgesetz (geändert 2000)
		1998	Nationale Grundsätze für einen fairen Umgang mit personenbezogenen Daten
		2002	Änderungsbestimmungen zum Datenschutz (Privatsektor)
	Neuseeland	1993	Privatsphäre-Schutzgesetz
Afrika	Südafrika	2014	Gesetz zum Schutz personenbezogener Daten
	Tunesien	2004	Gesetz zum Schutz personenbezogener Daten
	Senegal	2008	Gesetz zum Schutz personenbezogener Daten
	Mauritius	2004	Datenschutzgesetz

Die Verfassung ist das grundlegende und höchste Gesetz eines Landes und hat die höchste Rechtskraft und Autorität im Rechtssystem eines Landes. Der rechtliche Schutz personenbezogener Daten ist kein neues Thema. Aber es ist in der Tat ein relativ neues Thema, verschiedene Wege, Modelle und Methoden, die in verschiedenen Ländern zum Schutz der Datenrechte eingeschlagen oder verwendet wurden, aus verfassungsrechtlicher Sicht zu vergleichen und zu untersuchen. Die Vereinigten Staaten, Deutschland und Japan haben einen ausgereifteren Verfassungsschutz für Datenrechte. Frankreich ist am wahrscheinlichsten das Land, das den Schutz personenbezogener Daten in seiner Verfassung verankern wird.¹ Aufgrund der unterschiedlichen Geschichten, Kulturen und Rechtstraditionen gibt es große Unterschiede in den Konzepten, Methoden und

1 Die in Frankreich ansässige „European Times“ berichtete am 23. Juli 2018, dass die französische Nationalversammlung in der Nacht des 18. Juli Ortszeit für die Annahme einer Änderung gestimmt habe, um eine Klausel zum Schutz personenbezogener Daten in den Gesetzentwurf zur Änderung der Verfassung aufzunehmen. Die Klausel mit dem Titel „Bekämpfung der Ausweitung oder unangemessenen Verwendung personenbezogener Daten“ wird in Artikel 34 der Verfassung aufgenommen.

Wirksamkeiten des verfassungsmäßigen Schutzes von Datenrechten in verschiedenen Ländern. Es ist von großer Bedeutung für Verbesserung des verfassungsmäßigen Schutzes von Datenrechten in China, diese zu vergleichen und zu untersuchen (Yao Yuerong 2011, S. 70–76).

1. Vereinigte Staaten

Im Kontext der US-Gesetze entspricht die Diskussion über das Recht auf personenbezogene Daten der Diskussion über das Recht auf Privatsphäre. Obwohl das „Privatsphäre-Schutzgesetz“ von 1974 das Wort „Privatsphäre“ im Titel enthält, konzentriert sich sein Inhalt jedoch auf personenbezogene Daten und gilt als klassisches Gesetz zum Schutz der personenbezogenen Daten der Bürger im Bereich der öffentlichen Verwaltungsmacht. Um den Schutz der Datenrechte in den Vereinigten Staaten zu erörtern, müssen wir daher zuerst vom Recht auf Privatsphäre ausgehen.² Die Privatsphäre wurde zuerst im Bereich der

- 2 Es wird allgemein geglaubt, dass die Privatsphäre als eine der anerkannten Arten von Recht, das mit dem „alleinstehenden Recht“ im Buch „Über das Recht auf Privatsphäre“ von Warren und Brandeis (1890) begann. Beide Richter waren der Ansicht, dass jede Person das Recht hat, ob Dinge in seinem Besitz offengelegt werden und dass kein anderer das Recht hat, seine Produktionen ohne seine persönliche Zustimmung in irgendeiner Form zu veröffentlichen. In Entlehnung wird das übliche Beispiel der Verhinderung der Veröffentlichung von Manuskripten oder Kunstwerken durch andere verwendet, um zu argumentieren, dass dieses Recht zweifellos die Natur eines Eigentumsrechts hat. Wenn der Wert der Produktion jedoch nicht im Recht liegt, die aus der Veröffentlichung resultierenden Gewinne mitzunehmen, ist es schwierig, das Recht als eines von Eigentum in der gemeinsamen Akzeptanz dieses Begriffs zu betrachten, sondern geht es darum, die Bedrohungen des Seelenfriedens oder der Erleichterung, die sich aus jeglicher Veröffentlichung ergeben, zu verhindern. Das Prinzip, das persönliche Schriften und alle anderen persönlichen Produktionen nicht vor Diebstahl und physischer Aneignung, sondern vor Veröffentlichung in irgendeiner Form schützt, ist in Wirklichkeit nicht das Prinzip des Privateigentums, sondern das einer unantastbaren Persönlichkeit. Das Prinzip des Schutzes ist gerade das Recht auf Privatsphäre. Das Recht eines Privatpersonals, seine Privatsphäre zu schützen und die Veröffentlichung zu verhindern, ist der einfachste Fall für eine solche Ausweitung. Der Schutz des Rechts auf Privatsphäre ist ausdrücklich im letzten Band des ersten Restatement of Tort von 1939 enthalten.

zivilrechtlichen unerlaubten Handlung erörtert, aber mit dem Anliegen des Schutzes der Privatsphäre begann der Oberste Gerichtshof der USA mit der Auslegung des Rechts auf Privatsphäre in der Verfassung auf der Grundlage der vierten und fünften Änderung der Verfassung, und dann erweiterten die Richter ihre Auslegungsbefugnis auf die erste und die vierzehnte Änderung. Beispielsweise sind sie der Meinung, dass jede rechtswidrige Verletzung des Rechts auf Privatsphäre seitens des Staates als Verstoß gegen die vierte Änderung der Verfassung gilt. Ein weiteres Beispiel ist die Ausweitung der Vereinigungsfreiheit in der ersten Änderung zum Schutz der Privatsphäre von Verbandsmitgliedern. Der Oberste Gerichtshof der USA erkannte das Recht auf Privatsphäre als ein in der Verfassung vorgesehenes Recht an. Obwohl dies in der Verfassung nicht ausdrücklich vorgesehen ist, handelt es sich nach wie vor um ein Recht, das durch die Verfassungsänderung in ihrem Verzweigungsbereich ausgestattet ist und in den schattierten Geltungsbereich der Verfassungsrechte fällt und den unvermeidlichen Anforderungen eines ordnungsgemäßen Rechtsprozesses unterliegen muss. Die Behandlung des Rechts auf Privatsphäre als eigenständiges Verfassungsrecht ergibt sich jedoch aus der Auslegung der neunten Änderung.³ Es ist erwähnenswert, dass in den Vereinigten Staaten Verfassungsfälle, die sich direkt auf Datenrechte beziehen, relativ selten sind, während die Praxis des Schutzes von Datenrechten durch Gesetzgebungsverfahren aber große Erfolge erzielt hat (siehe Tabelle 5-2).

1960 schrieb Dean Prosser eine der einflussreichsten Veröffentlichungen des 20. Jahrhunderts mit dem Titel „Datenschutz“, durch Kämmen von mehr als 300 Fällen, die von den Berufungsgerichten im Zusammenhang mit Datenschutzstreitigkeiten entschieden wurden, die die Existenz der Privatsphäre im amerikanischen Rechtssystem bestätigen sind.

3 Die neunte Änderung ist eine allgemeine Bestimmung der Verfassung der Vereinigten Staaten, in der es heißt: „Die Aufzählung bestimmter Rechte in der Verfassung darf nicht so ausgelegt werden, dass andere Rechte, die vom Volk behalten werden, gezeugnet oder herabgesetzt werden können“.

Tabelle 5-2 Datenrechtsgesetzsystem der Vereinigten Staaten

Jahr	Gesetz	Beschreibung
1970	Fair Credit Reporting Act	Den Verbrauchern das Recht gegeben, Fehler zu korrigieren, und stellt sicher, dass Fehler in den Kreditauskünften der Verbraucher nicht dazu verwendet werden, den Verbrauchern Schaden zuzufügen.
1974	Datenschutzgesetz	Einzelpersonen das Recht gegeben, zu konsultieren, um die Richtigkeit der persönlichen Informationsdateien und die Richtigkeit der Informationserfassungszwecke sicherzustellen. Geheime Akten dürfen nicht aufbewahrt werden, und Einzelpersonen haben möglicherweise Zugang zu Rechtsbehelfen gegen Zivilprozesse.
1978	Finanzdatenschutzgesetz	Finanzinstitute sind verboten, die Finanzunterlagen der Kunden beliebig an die Bundesregierung weiterzugeben, ohne die Kunden zu informieren oder die Zustimmung der Kunden einzuholen. Die Bundesregierung muss bestimmte Verfahren einhalten und entsprechende Belege vorlegen, um die Finanzunterlagen der Kunden zu erhalten.
1980	Finanzdatenschutzgesetz	Die Anfrage von Finanzinstituten der Bundesregierung nach Bankunterlagen wurde geregelt.
1980	Datenschutzgesetz	Standards für Strafverfolgungsbehörden zur Verwendung von Informationen, die in Zeitungen und anderen Medien aufgezeichnet wurden, festgelegt.
1984	Gesetz über Kabelkommunikationsrichtlinien	Es sieht vor, dass ein Hinweis bereitgestellt werden muss, um persönliche Informationen zu erhalten, und dass Einzelpersonen das Recht haben, die dokumentierten Informationen zu überprüfen und die Bereitstellung irrelevanter Informationen zu verweigern.
1986	Datenschutzgesetz für elektronische Kommunikation	Umstände und Verbindlichkeiten einer Verletzung der Privatsphäre durch Abfangen oder Offenlegung von gespeicherten Kommunikationsinformationen wurden festgelegt.

(Fortsetzung)

Tabelle 5-2 Fortsetzung

Jahr	Gesetz	Beschreibung
1988	Gesetz zum Schutz der Video-Privatsphäre	Festlegung der Gewährleistung des sicheren Privatsphäre-Schutzes bei Kauf und Verleihung von Videobändern.
1994	Gesetz zum Schutz der Privatsphäre des Fahrers	Es legt Beschränkungen für die Verwendung und Offenlegung persönlicher Fahrzeugdaten durch staatliche Transportabteilungen fest.
1996	Gesetz über die Portabilität und Rechenschaftspflicht von Krankenversicherungen	Es schützt persönliche Gesundheits- und Datenschutzinformationen und verhindert die unbefugte Verwendung und Offenlegung.
1999	Gesetz zur Modernisierung von Finanzdienstleistungen	Finanzinstitute müssen die Privatsphäre und die persönlichen Daten der Verbraucher schützen.
2000	Gesetz zum Schutz der Online-Privatsphäre von Kindern	Es schützt persönliche Informationen, die von Onlinedienstleistern verarbeitet werden. Ohne Zustimmung der Eltern beschränken die Gesetze und Vorschriften des Bundes die Erfassung und Verwendung personenbezogener Daten von Kindern.
2008	Gesetz zur Nichtdiskriminierung Gen-Informationen	Es bietet einen verbesserten Schutz für die Privatsphäre und genetische Informationen.
2010	Gesetz zum finanziellen Verbraucherschutz	Es ermächtigt das Consumer Financial Protection Bureau, die finanzielle Privatsphäre zu überwachen und zu schützen.
2018	California Consumer Privacy Act	Der Anwendungsbereich wurde erheblich erweitert, und es wurde eine Reihe von Datenschutzrechten für Verbraucher in Bezug auf den Zugang zu, die Löschung und den Austausch von personenbezogenen Daten, die von Unternehmen gesammelt wurden, geschaffen, sodass Unternehmen strengere Maßnahmen zum Schutz personenbezogener Daten ergreifen müssen.

2. Deutschland

Als ein wichtiger Zweig des traditionellen kontinentalen Zivilrechtssystems unterscheidet sich die Rechtstradition und -kultur Deutschlands offensichtlich von der der Vereinigten Staaten. Der amerikanische Schutz personenbezogener Daten auf Privatsphäre-Ebene hat keine Flamme in Deutschland gezündet. „Im Zivilrecht oder in der Verfassung Deutschlands gibt es keinen Begriff von Recht auf Privatsphäre. Das Äquivalent zur Privatsphäre im US-Rechtssystem entspricht etwa der in der deutschen Rechtsprechungslehre genannten „Private Sphäre“ oder „Private Natur“.⁴ Das Recht auf Privatsphäre hat keinen Platz in der Rechtstradition Deutschlands, aber Deutschland ignoriert nicht die Theorien, Lehren und Präzedenzfälle im Zusammenhang mit dem Recht auf Privatsphäre, die in den Vereinigten Staaten mehr Anerkennung gefunden haben. Generell entspricht der Begriff des Schutzes der Persönlichkeitsrechte im privaten Bereich in Deutschland in seinem Zivilrechtssystem dem Konzept des Schutzes der Privatsphäre im Bereich der zivilrechtlichen unerlaubten Handlung in den Vereinigten Staaten, während der Schutz personenbezogener Daten und der Schutz der allgemeinen Handlungsfreiheit dem Schutz der Privatsphäre auf Ebene der Verfassung der Vereinigten Staaten entsprechen sollte. Das vom Bundesverfassungsgericht festgelegte und durch spezifische Bestimmungen des Bundesgesetzes über den Schutz personenbezogener Daten geschützte Recht auf Selbstbestimmung von Informationen gilt als das deutsche Gegenstück zum Schutz des Rechts auf Privatsphäre in den USA. Das Bundesverfassungsgericht hat auf der

4 Die deutsche Wissenschaftswelt hält seit Langem an der sogenannten „Sphärentheorie“ fest, in der personenbezogene Informationen entweder zur Privatsphäre oder zur Öffentlichkeit gehören. Diejenigen im privaten Bereich ähneln hier der Privatsphäre. Das Bundesverfassungsgericht hat in seinen Rechtsprechungen die Dinge auch in drei Kategorien unterteilt: die im Bereich der Privatsphäre, die im privaten Bereich und die im öffentlichen Bereich. Diese Theorie weist eine konzentrische Struktur auf, in der verschiedene Bereiche des Privatlebens Kreise mit unterschiedlichen Radien bilden und der Schutz auf der Grundlage der Abstände zum Zentrum gewährt wird. Wang Tze-chien: „Thema und Ausblick des Schutzes des Persönlichkeitsrechts (III) – das Recht der Privatsphäre“, (Band I), in „Regionale Rechtskunde in Taiwan“, 2007, 96. Ausgabe

Grundlage der vom Bundesgericht angenommenen Sphärentheorie die verfassungsrechtlichen Auslegungen zum Datenschutzbereich im privaten Bereich, der den Kern des absoluten Schutzes darstellt, gebilligt. Es wird betont, dass die Menschenwürde unantastbar sein muss und dass die Achtung und der Schutz der Menschenwürde die Pflicht aller staatlichen Machtbehörden sind, wie dies in Artikel 1 Absatz 1 des Grundgesetzes vorgesehen ist (Wang Tze-chien 2007).⁵ Anders als der US-amerikanische Ansatz zur Wahrung der Privatsphäre, der durch Ansprüche wie das „Recht auf Ruhe“, „Nichteinmischung in das Privatleben“ oder „Schweigen“ dargestellt wird, befasst sich Deutschland mit der theoretischen Perspektive des Schutzes des „Privatbereichs“, was bedeutet, dass alle Rechte wie die Unverletzlichkeit der persönlichen Freiheit nach Artikel 2 und die Glaubens- und Gedankenfreiheit nach Artikel 4, der Schutz der Privatsphäre in Korrespondenz, Post und Telekommunikation nach Artikel 10 und die Unverletzlichkeit des Wohnungseigenheims nach Artikel 13 usw. als Grundrechte der Persönlichkeit und Privatsphäre gelten. Gleichzeitig könnten die Presse-, Wissenschafts- und Kunstfreiheit nach Artikel 5 „Grundgesetz“ der besondere Schutz der Familie nach Artikel 6, die Versammlungsfreiheit nach Artikel 8 und die Vereinigungsfreiheit nach Artikel 9 in gewissem Umfang auch zum Schutz der Privatsphäre genutzt werden. Dieser Schutz der Grundrechte im privaten Bereich auf verfassungsrechtlicher Ebene ist jedoch nicht der gesamte Schutz. In der deutschen Theorie und Praxis werden die Menschenwürde in Artikel 1 Absatz 1 und die Persönlichkeitsrechte in Artikel 2 Absatz 1 des Grundgesetzes zur Auslegung und zum Schutz von Grundrechten herangezogen, die nicht aufgeführt sind, aber dennoch sollen die unbestimmten Rechtsinhalte, die zum Schutz der Grundrechte im privaten Bereich gehören, dargelegt und geschützt werden. Man kann sagen, dass der Schutz der Privatsphäre im Grundgesetz praktisch lückenlos ist und über ein dichtes und erweiterbares System zum Schutz der Grundrechte verfügt (siehe Tabelle 5-3).

5 Das „Grundgesetz“, d.h. das „Grundgesetz der Bundesrepublik Deutschland“, ist die Verfassung der Bundesrepublik Deutschland und das fundamentale Großgesetz Deutschlands.

Tabelle 5-3 Datenrechtsgesetzsystem Deutschlands

Jahr	Gesetz	Beschreibung
1970	Datenschutzgesetz des Landes Hessen	Als weltweit erstes Datenschutzgesetz hat es eine neue Ära des Datenschutzes durch Gesetzgebung eingeleitet.
1976	Bundesgesetz über den Schutz personenbezogener Daten	Das Gesetz, das 1977 in Kraft trat, ist offiziell als Gesetz zum Schutz vor dem Missbrauch personenbezogener Daten bei der Datenverarbeitung und allgemein als Gesetz zum Schutz personenbezogener Daten bekannt.
1977	Bundesdatenschutzgesetz	Es ist das weltweit erste, das ein einheitliches Regulierungsmodell für öffentliche und private Institutionen festlegte. Sowohl öffentliche als auch private Einrichtungen müssen personenbezogene Daten schützen, um eine umfassende Abdeckung des Schutzes personenbezogener Daten zu erreichen.
1997	Gesetz über Spezifikation der Informations- und Kommunikationsdienste	Auch als „Multimedien-Gesetz“ bekannt. Das ist weltweit das erste Gesetz, das sich mit der Kommunikation im Internet befasst. Sein Einfluss auf die Internetaufsicht in Deutschland spiegelt sich hauptsächlich in drei Aspekten wider: Erstens hat er die Ermittlung der Verbindlichkeiten für die illegale Kommunikation von Inhalten gestärkt; Zweitens beauftragt sie eine spezifische „Cyberpolizei“, die Verbreitung schädlicher Inhalte durch Gesetze und Vorschriften zu überwachen. Drittens gilt es als rechtswidrige Handlung, wenn eine Person im Internet schädliche Aussagen für Kinder macht oder verbreitet.

(Fortsetzung)

Tabelle 5-3 Fortsetzung

Jahr	Gesetz	Beschreibung
1997	Telekommunikationsdienstgesetz	Internetdiensteanbieter sind für die von ihnen bereitgestellten Inhalte gemäß den allgemeinen Gesetzen verantwortlich. Unter der Bedingung, dass der Diensteanbieter nicht gegen die Bestimmungen des Telekommunikationsgesetzes zur Geheimhaltung von Telekommunikationsgeheimnissen verstößt, ist er verpflichtet, die gesetzlich vorgeschriebene Weitergabe illegaler Inhalte zu verhindern. Wenn es Beweise dafür gibt, dass die dem Diensteanbieter bekannten Informationen illegale Inhalte enthalten, deren Verbreitung technisch verhindert werden kann, dies jedoch nicht getan, handelt es sich um eine „vorsätzliche Verletzung“, und der Diensteanbieter „muss die gesamtschuldnerischen Verpflichtungen für die illegalen Aktivitäten tragen“.
1997	Telekommunikationsdatenschutzverordnung	enthält strenge Bestimmungen für mögliche Verstöße gegen personenbezogene Daten während des Internetbetriebs.
2007	Telemediengesetz (im Jahr 2010/2016/2017 nacheinander überarbeitet)	Als Kernstück der deutschen Internetgesetzgebung ist dieses Gesetz allgemein als „Internetgesetz“ bekannt. „Telemedien“ ist ein einzigartiger Begriff im deutschen Medienrecht und deckt nahezu alle Arten von Internetdiensten in Deutschland ab.

3. Japan

Japan hat das westliche System bereits in der Meiji-Ära in seine Reformen eingeführt und sein Rechtssystem wurde daher stark von Kontinentaleuropa und insbesondere von den deutschen politischen, militärischen und rechtlichen Systemen beeinflusst, die fast vollständig kopiert wurden. Nach dem Zweiten Weltkrieg „übernahmen“ die Vereinigten Staaten

Japan und stellten es unter ihre alleinige Kontrolle. Die japanische Verfassung wurde daher von den Amerikanern entworfen, aber im Namen der japanischen Regierung verkündet. Der gesamte Prozess wurde von den Amerikanern geleitet (Li Wei 2009). Dies ist der verständliche Grund dafür, dass auch im heutigen japanischen Rechtssystem traditionelle Elemente aus Deutschland und den USA integriert sind. Das ist gerade die Eigenheit des japanischen Rechtssystems. Personenbezogene Daten der Bürger wurden zunächst aus Sicht der Privatsphäre geschützt. 1970 veröffentlichte Professor Koji Sato die „konstitutionelle Position zum Datenschutz (auf der Ebene des öffentlichen Rechts)“, die auf der amerikanischen Datenschutztheorie beruhte und nach einer verfassungsmäßigen Grundlage für das Recht auf Privatsphäre aus dem in Artikel 13 der japanischen Verfassung garantierten „Recht auf Streben nach Glück“ sucht. „Nach japanischem Recht wird das Recht auf Privatsphäre hauptsächlich unter dem Gesichtspunkt geschützt, das Recht zu betonen, die Offenlegung eigener persönlicher Informationen oder persönlicher Angelegenheiten zu verweigern, während andere persönliche Interessen wie Namen, Porträts, Bereiche des persönlichen Lebens und Selbstbestimmung durch Auslegung des Rechts auf Streben nach Glück in gewissem Maße geschützt werden sollen.“ In Artikel 13 der Verfassung Japans heißt es: „Alle Bürger sind als Individuum zu respektieren. Ihr Recht auf Leben, Freiheit und Streben nach Glück wird in dem Maße, in dem es das Gemeinwohl nicht beeinträchtigt, in der Gesetzgebung und in anderen Regierungsangelegenheiten oberste Priorität haben.“ Diese Bestimmung wird oft als Bestimmung zur „persönlichen Würde“ bezeichnet, und die persönliche Würde wird als eines der in der japanischen Verfassung festgelegten Grundrechte angesehen. Das Recht auf Streben nach Glück war ursprünglich ein allgemeiner Begriff für Menschenrecht der Einzelperson, aus dem keine anderen Rechte direkt abgeleitet werden konnten. Bis in die 1960er-Jahre, da die sozialen und wirtschaftlichen Turbulenzen mehr Herausforderungen mit sich brachten, sollte die Auslegungsbedeutung dieser Bestimmung neu bewertet werden. „Infolgedessen wurde das Recht auf Streben nach Glück, basierend auf dem Prinzip der Achtung des Individuums, nach und nach als ein allgemeines Recht interpretiert, das neue Menschenrechte untermauert, die nicht in der Verfassung aufgeführt sind“ (Nobuyoshi Ashibe 2006, S. 104).

Tabelle 5-4 Datenrechtsgesetze Japans

Jahr	Gesetz	Beschreibung
1973	Bestimmungen der Stadt Tokushima in Bezug auf das Management personenbezogener Daten auf Computern	Gesetzgebende Spezifikation des Respekts der Achtung der Rechte und Interessen der Privatsphäre, die mit der Verarbeitung personenbezogener Daten durch Regierung verbunden sind.
1988	Gesetz zum Schutz personenbezogener Daten im Zusammenhang mit der elektronischen Datenverarbeitung durch Verwaltungsorgane	Der Schutzzumfang beschränkt sich auf personenbezogene Daten, die von Computern verarbeitet werden, und umfasst keine manuell verarbeiteten Dateninformationen.
1997	Richtlinien zur Computerverarbeitung und zum Schutz personenbezogener Daten im privaten Sektor	Erteilung von Datenschutz-Zertifizierungszeichen an Unternehmen mit wirksamen Schutzmaßnahmen (P-MARK-Zertifizierung)
2003	Gesetz zum Schutz personenbezogener Daten und unterstützende Gesetzreihe wie das Gesetz zum Schutz personenbezogener Daten im Zusammenhang mit der elektronischen Datenverarbeitung durch Verwaltungsorgane, das Gesetz zum Schutz personenbezogener Daten von eingetragenen Verwaltungsbehörden usw., Offenlegung von Informationen und Überprüfung des Schutzes personenbezogener Daten, Gesetz zur Festlegung des Ausschusses, Gesetz zur Verbesserung einschlägiger Gesetze, die an der Umsetzung des Gesetzes über den Schutz personenbezogener Daten von Verwaltungsorganen beteiligt sind	Das „Gesetz zum Schutz personenbezogener Daten“ wird als Grundgesetz zum Schutz personenbezogener Daten in verschiedenen Bereichen bezeichnet und wird allgemein als „Fünf Koordinierungsgesetze zum Schutz personenbezogener Daten“ mit den anderen vier Gesetzen bezeichnet.

Tabelle 5-4 Fortsetzung

Jahr	Gesetz	Beschreibung
2015	Gesetz zum Schutz personenbezogener Daten (überarbeitet)	Erweiterung des Anwendungsbereichs des Schutzes personenbezogener Daten und der Anwendung von Gesetzen und Förderung der Anwendung anonymer personenbezogener Daten.

(II) Vergleich der Gesetzgebung zur Datensicherheit

Datensicherheit ist eine wichtige Grundlage und Komponente des Datenrechtsschutzes. Die Europäische Union, die Vereinigten Staaten, Japan, Australien, Russland, Singapur und andere Länder mit gut entwickelten Datenschutzsystemen haben diesbezüglich eine Reihe von Gesetzen und Vorschriften erlassen (siehe Tabelle 5-5). Obwohl sie unterschiedliche Strategien und Ansätze bei der diesbezüglichen Gesetzgebung verfolgen, sind die in ihren einschlägigen Gesetzen und Vorschriften enthaltenen Hauptelemente im Wesentlichen dieselben. Durch Zusammenfassung und Prüfung der einschlägigen Gesetze und Vorschriften der Europäischen Union, der Vereinigten Staaten, Japans und anderer Länder sowie durch Analyse und Beurteilung der in ihrer Gesetzgebung zur Datensicherheit enthaltenen Grundprinzipien können wir unser Verständnis der verschiedenen Gesetzgebungsmodelle und -konzepte vertiefen und anschließend Ratschläge zu unserer Datensicherheitsgesetzgebung erhalten sowie wichtige Informationen für Formulierung spezifischer Datenschutzgesetze, -vorschriften, Verwaltungsvorschriften und Branchenstandards in China bereitstellen.⁶

6 Siehe Nationales Technisches Komitee für Standardisierung der Informationssicherheit, Sonderarbeitsgruppe – Big-Data-Sicherheit: Weißbuch zur Standardisierung der Big-Data-Sicherheit (Ausgabe 2018), 16. April 2018. <<http://www.cesi.cn/201804/3789.html>>.

I. Europäische Union

Die Gesetzgebung zur Datensicherheit in der Europäischen Union verfolgt einen staatlich geführten Ansatz. Die Mitgliedstaaten der EU sind der Ansicht, dass personenbezogene Daten die Merkmale von Persönlichkeitsrechten aufweisen, die Konnotation von Persönlichkeitsrechten widerspiegeln, durch die in der Verfassung verankerten Grundrechte abgedeckt und im Rahmen der in bestimmten AbteilungsGesetzen vertretenen materiellen Rechte geregelt und geschützt werden sollen. Als Organisation der regionalen politischen und wirtschaftlichen Integration ist die Europäische Union relativ stark in der Gesetzgebung integriert, bietet auch Raum für die selbstständige Entwicklung ihrer Mitgliedstaaten und bildet ein großes Muster aus EU-Gesetzen und Gesetzen der Mitgliedstaaten. Zunächst werden auf der EU-Ebene programmatische Leitlinien für rechtliche Fragen im Zusammenhang mit der Datensicherheit erstellt. Zu diesen Rechtsdokumenten gehören z.B. Konventionen, Richtlinien, Leitlinien, Rahmenvereinbarungen usw. Der Inhalt dieser programmatischen Rechtsdokumente ist möglicherweise nicht direkt auf bestimmte Rechtspraktiken anwendbar, hat jedoch den Grundrahmen und die Grundprinzipien für Gesetzgebung zur Datensicherheit in Mitgliedstaaten festgelegt. Nach diesem Muster formuliert jeder Mitgliedstaat seine eigenen Gesetze und Vorschriften zum Datensicherheitsschutz. Aufgrund seiner Vollständigkeit, Strenge und Durchführbarkeit hat der rechtliche Schutz der Sicherheit personenbezogener Daten in der Europäischen Union weltweit großen Einfluss. Auf der EU-Ebene wurde seit 1981 eine Reihe von Dokumenten wie das „Übereinkommen zum Schutz der persönlichen Informationen bei der automatischen Verarbeitung personenbezogener Daten“ (1981), „Beschluss des Rates vom 31. März 1992 im Bereich der Sicherheit von Informationssystemen“ (92/242 / EWG), „personenbezogene Datenschutzrichtlinie“ (1995), „Datenschutz- und elektronische Kommunikationsrichtlinie“ (2002), „Richtlinie zur Vorratsdatenspeicherung“ (2006), die „COMPACT Internet Verwaltungsgrundsätze der Europäischen Union“ (2011), „European Strategic Initiative“ (2012),

„Cyberraum-Sicherheitsstrategie“ (2013), die „Allgemeine Datenschutzverordnung“ (2018) sowie andere Rechtsdokumente einander folgend in Kraft gesetzt. Auf diese Weise wurden der Rechtsrahmen und die Grundnormen für den Datensicherheitsschutz in der EU geschaffen, der grenzüberschreitende Datenfluss wird schrittweise gesetzlich geregelt, und wurden auch einschlägige Regulierungs- und Aufsichtsbehörden für Schutz personenbezogener Daten von Internetbenutzern eingerichtet (Ran Congjing & Wang Bingjie 2019), und damit auch eine solide Grundlage für den Aufbau des „strengsten“ EU-Rechtsschutzsystems für Datensicherheit gelegt.

2. Vereinigte Staaten

Die Gesetzgebung zur Datensicherheit in den USA unterscheidet sich einigermassen von denen in der EU. Die Vereinigten Staaten haben keinen einheitlichen Rechtsrahmen für den Schutz personenbezogener Daten. Stattdessen ist der Schutz spezifisch für verschiedene Bereiche oder Angelegenheiten jeweils durch Gesetzgebung festgelegt. In den amerikanischen rechtlichen Regelungen für Datensicherheit sind personenbezogene Daten und Daten der Privatsphäre durch Verfassung, Datenschutzgesetze und andere rechtliche Dokumente geschützt, während wichtige Daten in wichtigen Branchen und Bereichen durch besondere Gesetze geschützt werden und allgemeine Daten durch branchenspezifische Selbstregulierung und Marktregulierung abgedeckt sind, die ein allgemeines Rechtsmuster bilden, in dem mehrere Parteien an der Regulierung der Datensicherheit beteiligt sind. Das Recht auf Privatsphäre ist die rechtsphilosophische Grundlage der Gesetzgebung zum Schutz der Sicherheit personenbezogener Daten in den Vereinigten Staaten. In gewissem Sinne entspricht die Konnotation des Rechts auf Privatsphäre in den Vereinigten Staaten der des Persönlichkeitsrechts im kontinentalen Zivilrechtssystem. Man kann sagen, dass das US-amerikanische Rechtssystem zum Schutz der Datensicherheit ein umfassendes System ist, das die Persönlichkeit der Datenrechtshaber schützt, was sich sowohl in den Gesetzen und Vorschriften zur

Sicherheit personenbezogener Daten des Landes als auch in den Vorschriften zur Branchenselbstregulierung widerspiegelt. Der Schutz personenbezogener Daten in den USA kann in den Schutz im öffentlichen Bereich und den Schutz im privaten Bereich unterteilt werden. So ist die Gesetzgebung im öffentlichen Bereich in dezentralisierter Form und im privaten Bereich durch Branchen-Selbstregulierungsmodell repräsentiert. Im öffentlichen Bereich gibt es folgende Gesetze zum Schutz der Datensicherheit: das Fair Credit Reporting Act (1971), das sich mit der Erhebung, Verarbeitung und Speicherung personenbezogener Daten durch private Organe befasst; das Privacy Act (1974), das sich mit der Verarbeitung personenbezogener Daten durch staatliche Organe befasst; Family Education Rights and Privacy Act (1976), das die persönlichen Daten von Schülern und ihren Eltern schützt; das Electronic Communications Privacy Act (1986) und das Computer Matching and Privacy Protection Act (1988), die sich mit der Verarbeitung elektronischer Informationen befassen; das Children's Online Privacy Protection Act (2000) zum Schutz der persönlichen Daten von Kindern etc. und das USA Freedom Act, das am 2. Juni 2015 verabschiedet und in Kraft getreten ist. Das Branchen-Selbstregulierungsmodell in den USA ist ein von der Regierung geführtes Selbstregulierungsmodell, was ein Ergebnis von wechselseitigen Dialogen zwischen und gemeinsamen Innovationsbemühungen von „Regierungen, Unternehmen, Universitäten, Forschungsinstituten und Benutzern“ darstellt. Es ist in bestimmtem Maße flexibel und behilflich und ergänzend zur Gesetzgebung. Dieses Modell wird auch als „Leitende Gesetzgebung“ bezeichnet (Zhao Qiuyan 2005). Insbesondere gibt es drei Hauptformen einer solchen Branchen-Selbstregulierung für Datensicherheit: Technologieschutz, Branchenanleitung und kommerzielle Zertifizierung. Beispielsweise wurde in dem 1995 von der Regierung der Vereinigten Staaten herausgegebenen „Rahmen für den globalen elektronischen Geschäftsverkehr“ klar darauf hingewiesen, dass die Regierung die Bemühungen kommerzieller Organisationen unterstützt, ein auf Selbstregulierung basierendes System einzurichten, um den wirksamen Schutz der Privatsphäre ihrer Kunden zu erleichtern.

3. Japan

Die Gesetzgebung zur Datensicherheit in Japan begann später als in Europa und Amerika. Aber Japan ist immer noch eines der ersten Länder in Asien, das Gesetze zum Schutz der Sicherheit personenbezogener Daten erlassen hat, und verfügt in dieser Hinsicht über ein relativ besser entwickeltes Rechtssystem. Japan hat Erfahrungen der EU-Gesetzgebung zur Datensicherheit gezogen und den Rechtsrahmen von der Europäischen Union übernommen. Das auf diese Weise gebildete umfassende System zum Schutz personenbezogener Daten, das sich auf die Persönlichkeits- und Eigentumsrechte der Bürger einschließlich ihres Rechts auf Privatsphäre konzentriert, regelt das Verarbeitungsverhalten personenbezogener Daten sowohl von Regierungsbehörden als auch von privaten Unternehmen. Gleichzeitig hat Japan bei seinen Gesetzgebungsbemühungen auch von pragmatischer Gesetzgebung der Vereinigten Staaten gelernt. Auf der Grundlage des Gesetzes zum Schutz personenbezogener Daten werden spezielle Gesetze, Selbstregulierung und Aufsicht durch Dritte für Schlüsselbranchen berücksichtigt, um ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Anwendung von Daten zu erreichen. Es ist zu unterstreichen, dass Japan in seiner Gesetzgebungspraxis und Festlegung zu Datenrechten viele Referenzen aus dem Ausland gezogen hat, ohne seine eigenen spezifischen Bedingungen und sein reales Umfeld zu ignorieren, und dass es das Gleichgewicht zwischen dem Schutz der legitimen Rechte und Interessen der Individuen und der Förderung des freien Datenflusses gebührend berücksichtigt. Wenn wir Japans Gesetzgebungsprozess im Bereich des Schutzes personenbezogener Daten überprüfen, können wir feststellen, dass die entsprechenden Bemühungen in den 1980er-Jahren mit einigen lokalen und industriellen Gesetzen und Vorschriften sowie Gesetzen zum Schutz personenbezogener Daten der Verwaltungsbehörden begonnen haben. Beispielsweise formulierte das JIPDEC (Information Processing Development Center) in Japan im März 1987 die „Richtlinien zum Schutz personenbezogener Daten in Finanzinstituten“ und im März 1988 die „Richtlinien zum Schutz

personenbezogener Daten im privaten Sektor“. 1989 formulierte das Ministerium für Wirtschaft, Handel und Industrie die „Richtlinien für Verarbeitung und Schutz personenbezogener Daten durch Computer im privaten Sektor“ (Xie Qing 2006). Zu Beginn des 21. Jahrhunderts hat Japan das „Gesetz zum Schutz personenbezogener Daten“⁷ 2003 offiziell erlassen und 2013 beschlossen, es zu ändern. Am 30. Mai 2017 trat das neu geänderte „Gesetz zum Schutz personenbezogener Daten“ offiziell in Kraft. „Diese neueste Version des ‚Gesetzes zum Schutz personenbezogener Daten‘ bietet einen detaillierteren Schutz des Rechts auf personenbezogene Daten und Änderungen im Zusammenhang mit der Verwendung anonymer Informationsverarbeitung, der Zertifizierung von Unternehmen für die Verwendung von Informationen, dem Zertifizierungssystem von Drittanbietern und der Übertragung von Befugnissen des Generalministers über Praktiker, die diese persönlichen Informationen erhalten, an die Kommission für Schutz persönlicher Informationen sind alles neue Errungenschaften bei der Verbesserung der Gesetzgebung zum Schutz persönlicher Informationen“ (Wei Jianxin & Song Renchao 2018).

7 „Fünf Gesetze zum Schutz personenbezogener Daten“, darunter das „Gesetz zum Schutz personenbezogener Daten“, das „Gesetz zum Schutz personenbezogener Daten von Verwaltungsorganen“, das „Gesetz zum Schutz personenbezogener Daten unabhängiger Verwaltungsrechtspersonen“ und das „Gesetz zur Offenlegung von Informationen – Gesetz zur Einrichtung einer Überprüfungskonferenz zum Schutz personenbezogener Daten“, „Gesetz zum Schutz personenbezogener Daten, die von Verwaltungsorganen gehalten werden“, werden zusammen als „Gesetz zum Schutz personenbezogener Daten“ bezeichnet.

Tabelle 5-5 Datensicherheitsgesetze und -bestimmungen der wichtigsten Länder

Land/ Region	Gesetze, Vorschriften und Abteilungsregeln	Jahr	Kategorie
Euro- päische Union	Datenschutz-Grundverordnung	2018	allgem. Recht
	EU-Richtlinie zur Vorratsdatenspeicherung	2006	allgem. Recht
	Datenschutz- und elektronische Kommunika- tionsrichtlinie	2002	allgem. Recht
	EU-Datenschutzrichtlinie	1995	allgem. Recht
Vereinigte Staaten	Privacy Shield-Protokoll	2016	allgem. Recht
	California Online-Datenschutzgesetz	2014	Landes- gesetz
	Bundesdatenschutzgesetz	2014	allgem. Recht
	Gesetz über digitale Rechenschaftspflicht und Transparenz	2014	Branchen- regel
	Strategie der digitalen Regierung	2012	allgem. Recht
	Offene Regierungsrichtlinie	2009	allgem. Recht
	Gesetz zur Benachrichtigung über Sicherheits- verletzungen in Kalifornien	2002	Landes- gesetz
	Gesetz zur Modernisierung von Finanzdienst- leistungen	1999	Branchen- regel
	Gesetz über Portabilität und Rechenschafts- pflicht von Krankenversicherungen	1996	Branchen- regel
	Bundesgesetz über die Handelskommission	1914	Branchen- regel

(Fortsetzung)

Tabelle 5-5 Fortsetzung

Land/ Region	Gesetze, Vorschriften und Abteilungsregeln	Jahr	Kategorie
Japan	Gesetz zum Schutz personenbezogener Daten (Änderung)	2017	allgem. Recht
	Gesetz zum Schutz personenbezogener Daten	2005	allgem. Recht
	Gesetz zum Schutz personenbezogener Daten in Bezug auf elektronische Datenverarbeitung durch Verwaltungsorgane	1988	allgem. Recht
	Richtlinien zum Schutz computergestützter Daten	1976	allgem. Recht
Australien	Telekommunikationsgesetz	1997	Branchenregel
	Bundesdatenschutzgesetz	1988	allgem. Recht
Russland	Artikel 152-FZ des Gesetzes der Russischen Föderation über personenbezogene Daten 2006	2015	allgem. Recht
	Artikel 149-FZ des Gesetzes der Russischen Föderation über Information, Informationstechnologie u. Datenschutz 2006	2006	allgem. Recht
	Straßburger Übereinkommen	2005	allgem. Recht
Singapur	Gesetz zum Schutz personenbezogener Daten	2012	allgem. Recht

Quelle: Siehe Nationales Technisches Komitee für Informationssicherheitsstandardisierung, Arbeitsteam für Big-Data-Sicherheitsstandards: Weißbuch zur Standardisierung von Big-Data-Sicherheit (Ausgabe 2018), 16. April 2018. <<http://www.cesi.cn/201804/3789.html>>.

(III) Vergleich der Regierungsverwaltungssysteme

Daten werden zu einer wichtigen Triebkraft für Innovationen in der Regierungsverwaltung und drängen auf Veränderungen von Regulierungsidee, -modell, -inhalt und Verwaltungsmittel etc. durch Regierungen. Die digitale Regierung wird zu einer wichtigen Manifestationsform von Konzepten wie ganzheitlicher Regierung, offener Regierung, synergetischer Regierung, dienstleistungsorientierter Regierung und intelligenter Regierung. Eine von Daten getriebene Regierung wird historische Veränderungen in der Regierungsverwaltung bewirken, die Modernisierung der Regierungsverwaltung nachdrücklich unterstützen und als Weg zur Realisierung der Modernisierung der Regierungsverwaltung dienen. Im Zeitalter von Big Data denken alle Regierungen sowohl von Industrials als auch von Entwicklungsländern über Regierungsumwandlungen und den Aufbau von Regierungsverwaltungssystemen nach (siehe Tabelle 5-6). Die Europäische Union, die Vereinigten Staaten und Japan sind Vorreiter und Marktführer im Bereich „Big Data plus Regierungsverwaltung“ und sie profitieren auch viel von solchen Bemühungen. Für China und andere Entwicklungsländer ist es von großer realistischer Bedeutung, die digitalisierte, internetvernetzte und intelligente Entwicklung der Regierungsverwaltung zu fördern, indem wir die datengetriebenen Regierungsverwaltungssysteme dieser drei Länder vergleichen und sorgfältig untersuchen, um die Unterschiede zwischen diesen herauszufinden und eine Reihe neuer Mechanismen zusammenzustellen, deren „Offenlegung, Entscheidungsfindung, Verwaltung und Innovation auf Daten“ basieren.

1. Europäische Union

Die E-Verwaltung ist der Ausdruck des neuen Merkmals, das die E-Regierung (oder E-Regierungsführung) in ihrer späteren Entwicklungsphase darstellt.⁸ Sie steht auch für neue Untersuchungen der

8 Wie ein niederländischer Wissenschaftler Michael Backes betonte, bezieht sich E-Verwaltung auf das Verwaltungsmodell, das mithilfe von Informationstechnologie

Europäischen Union zur Modernisierung ihres Regierungsverwaltungssystems und Steigerung ihrer Regierungsfähigkeit. Im Vergleich zur Technologie spielt der Systemaufbau eine wichtigere Rolle bei der Entwicklung von E-Verwaltung. Im Dezember 2005 wurden in der vom Ministerrat der Europäischen Union eingeführten Ministererklärung in Manchester zu E-Regierung vier Arbeitsprioritäten für die anfängliche Entwicklung der E-Verwaltung vorgeschlagen: alle Bürger einzuschließen, Arbeitseffizienz der Regierungsstelle zu steigern, öffentliche Dienstleistungen bereitzustellen, die die Nachfrage der Kunden klar widerspiegeln und einfachen und erweiterten Zugang zu öffentlichen Online-Diensten für Bürger aller Mitgliedstaaten durch ein gemeinsam anerkanntes Zertifizierungssystem anzubieten. Im Jahr 2006 veröffentlichte die Europäische Kommission den „i2010-E-Regierungsaktionsplan zur Beschleunigung des Aufbau der elektronischen Regierung in Europa zum Nutzen aller“, der Teil der Gesamtstrategie der EU zur Informatisierung i2010 ist. Die Bekanntgabe und Umsetzung dieses Aktionsplans kennzeichnet, dass der Aufbau von E-Regierung auf europaweiter Ebene auf den Weg zur systematischen Entwicklung gebracht ist.⁹ Das

den Prozess der Regierungsverwaltung und der öffentlichen Angelegenheiten vereinfacht und die Demokratisierung im Zusammenspiel von Regierung und Zivilgesellschaft, Regierung und Unternehmen sowie Regierungsoperationen fördert. Die Interpretation des Hauptberichts der 26. Internationalen Konferenz für Verwaltungswissenschaften lautete wie folgt: E-Verwaltung ist keine einfache Anwendung neuer Informations- und Kommunikationstechnologien im Bereich der öffentlichen Angelegenheiten, sondern eine Art gesellschaftlich-politischen Organisationen und ihre Handlungsweise, die mehr mit der Art und Weise der Organisation und Nutzung politischer Macht und sozialer Macht im Zusammenhang steht und ist die Ausdrucksweise von Verwaltung im Informationszeitalter. Siehe Dong, Lisheng: „Systematische Analyse der Entwicklung der E-Verwaltung in EU“, in Journal der Parteschule des Stadtkomitees der KP Chinas Hangzhou, 2015, 5. Ausgabe.

9 „i2010 E-Regierungs-Aktionsplan – Beschleunigung des Aufbaus der E-Regierung in Europa zum Nutzen aller“. Die fünf Kernperspektiven der Beseitigung der digitalen Kluft, der Verbesserung der Effizienz, der Umsetzung des elektronischen Beschaffungswesens, der Einrichtung europaweiter E-Service-Kanäle, der Verbesserung der Beteiligung und der demokratischen Entscheidungsfindung, wie im Aktionsplan dargelegt, können als Konkretisierung der Erklärung des Ministerrates

E-Verwaltungsgesetz der Europäischen Union ist im Grunde ein Regulierungssystem. Neben den allgemeinen Rechtsdokumenten wie der „E-Commerce-Richtlinie“, der „Richtlinie zum rechtlichen Schutz von Datenbanken“ und der „Richtlinie zu bestimmten rechtlichen Aspekten im Binnenmarkt und im elektronischen Geschäftsverkehr“ (Richtlinie zum elektronischen Geschäftsverkehr) zielt das Regulierungssystem hauptsächlich auf Bereich der Entwicklung der E-Verwaltung ab, die einer strengen Kontrolle bedürfen. Wie im Hinblick auf die Gesundheit des Cyberspace führte das Vereinigte Königreich im September 1996 das „3R-Internetsicherheitsregeln“ ein, mit denen illegale, insbesondere pornografische und obszöne Materialien durch die grundlegenden Maßnahmen „klassifizierte Identifizierung, Berichterstattung und Anzeigen und Verantwortungsübernahme“ aus dem Cyberspace entfernt werden sollen. Das Cyberspace-Management in Frankreich legt großen Wert auf den Schutz von Minderjährigen. Zum Beispiel hat Frankreich 1998 das „Gesetz zum Schutz von Minderjährigen“ erlassen, das schwere und strenge Strafen für Nutzung des Internets zur Verführung von Jugendkriminalität vorsieht. Durch die Annahme des „Übereinkommens zum Schutz personenbezogener Daten im automatischen Verarbeitungssystem“, der „Richtlinie zum Schutz personenbezogener Daten bei der Verarbeitung personenbezogener Daten und des freien Datenverkehrs“, der „ersten Richtlinie zur Übermittlung von personenbezogenen Daten an Drittländer – Mögliche Programme zur Bewertung der Angemessenheit und des „Schutzes der Erhebung und Übermittlung personenbezogener Daten auf der Datenautobahn“ setzen strenge Standards für den Schutz der Privatsphäre von Personen im Internet.

2. Vereinigte Staaten

Offene Regierungsdaten stellen einen Durchbruch in der Verwaltungsreform der Vereinigten Staaten dar. Im Juli 1966 verabschiedete die US-Regierung das Freedom of Information Act, das „das Recht der Öffentlichkeit auf Erhalt von Verwaltungsinformationen und die Verpflichtung der Verwaltungsorgane zur Bereitstellung von Verwaltungsinformationen für die Öffentlichkeit“ vorsieht (Nationales Technisches

Komitee für Standardisierung der Informationssicherheit zu Big Data Sicherheitsstandardisierung 2017). Im September 1993 wurde Building the Information Superhighway veröffentlicht, mit dem die Revolution der Informationstechnologie eingeleitet und ein umfassendes Informationssystem mit dem Internet im Mittelpunkt eingerichtet wurde. Dadurch wurde das Modell der Regierungsverwaltung gründlich verändert. Im Dezember 2009 gab die US-Regierung die Richtlinie für offene Regierung heraus, startete data.gov für den Zugang zu öffentlichen Daten, legte die drei Prinzipien der offenen Regierung fest, d.h. „Transparenz, Beteiligung und Zusammenarbeit“, forderte die Regierung auf, Daten über die Website zu veröffentlichen, damit die Öffentlichkeit mehr über Regierungsangelegenheiten informiert wird, fördert öffentliche Dialoge und gibt der Öffentlichkeit mehr Vertrauen in die Regierung. Seitdem hat die US-Regierung das Konzept von „Big Data“ kreativ in den Bereich der Regierungsverwaltung eingeführt. „Im März 2012 veröffentlichte die US-Regierung die ‚Big-Data-Forschungs- und Entwicklungsinitiative‘, um ihr ‚Big-Data-Entwicklungsprogramm‘ offiziell zu starten. Sie kündigte an, mehr als 200 Millionen US-Dollar für Big-Data-Forschung auszugeben. Im Mai desselben Jahres gab die Bundesregierung dann die ‚Digitale Regierungsstrategie‘ bekannt, die darauf abzielt, dem amerikanischen Volk bessere ‚digitalisierte‘ Dienste zu bieten. Bald darauf folgte eine Reihe von Maßnahmen rund um Daten von der US-Regierung und die Auswirkungen von Big Data auf die US-Regierung wurden nach und nach sichtbar“ (Liu Yeting & Tang Sisi 2014). Die drei großen Ziele der Entwicklung digitaler Regierungen in den Vereinigten Staaten lauten wie folgt: „Erstens soll das amerikanische Volk überall und jederzeit auf irgendwelchem Gerät auf hochwertige digitale Regierungsinformationen und -dienste zugreifen können. Zweitens soll die Regierung Geräte, Anwendungen und Daten auf intelligente, sichere und erschwingliche Weise beschaffen und verwalten, um sicherzustellen, dass sich die Regierung an diese neue digitale Welt anpassen kann. Drittens soll die Funktion der Regierungsdaten weiterhin freigesetzt werden, um

der Europäischen Union über elektronische Regierungsdienste in Manchester im Dezember 2005 angesehen werden.

Innovationen im ganzen nationalen Bereich zu erregen und dadurch die Qualität der Dienstleistungen für das amerikanische Volk zu erhöhen (E-Regierungsforschungszentrum der Parteschule des Zentralkomitees der KP Chinas 2019).

3. Japan

Japan ist weltweit führend in der nationalen Regierungsführung. Mit fortschreitender Meiji-Restauration holte Japan innerhalb kurzer Zeit die europäischen und amerikanischen Mächte ein und übertraf sie sogar. Dadurch wurde es zum ersten Land in Asien, das den Modernisierungsprozess startete und abschloss, was als ein wichtiges typisches Beispiel für die Modernisierungsforschung diente. Die japanische Regierung richtete im Jahr 2000 das „strategische IT-Hauptquartier“ ein und startete 2001 die „E-Japan-Strategie“ mit dem Ziel, Japans Fähigkeit für die gesamte IKT-Infrastruktur zu steigern und Japan zum weltweiten Führer der IT-Entwicklung zu machen. Im Jahr 2003 verabschiedete die japanische Regierung die „E-Japan-Strategie II“, in der der Schwerpunkt und die Richtung der Entwicklung der japanischen Informatisierung in größerem Maße angepasst wurden, um die Anwendung von Informationstechnologien insbesondere in den sieben Bereichen wie Gesundheitswesen, Ernährung, Leben, Finanzen für kleine und mittlere Unternehmen, Bildung, Beschäftigung und Verwaltung usw. zu fördern. In der Zwischenzeit wurde vorgeschlagen, den hocheffizienten Einsatz von Informationstechnologien in fünf horizontalen Projekten auszuweiten, nämlich Infrastruktur der neuen Generation, Vertraulichkeit, Forschung und Entwicklung, Personalwesen und internationale Strategie (Liu Ziheng & Zhou Jiagui 2013). Im Dezember 2004 wurde die U-Japan-Politik¹⁰ ins Leben gerufen, die darauf abzielt, die japanische Regierung zu einer

10 Der Buchstabe U in der „u-Japan-Strategie“ hat hier vier Konnotationen: erstens allgegenwärtig (Ubiquitous), zweitens universal (Universal), drittens benutzerorientiert (User-oriented) und viertens einzigartig (Unique). Japans Ankündigung der U-Japan-Politik markiert eine neue Phase beim Aufbau seines E-Regierungsnetzwerks, d.h. von der E-Phase bis zur U-Phase.

verallgemeinerten Existenz zu machen, die zu jeder Zeit und an jedem Ort öffentliche Dienstleistungen für jedermann in jeder Angelegenheit erbringen kann. Im Januar 2006 gab die japanische Regierung erneut die „neue IT-Reformstrategie“ heraus, die den Aufbau von E-Regierung einen wichtigen Bestandteil davon machte. Im Juli 2009 wurde mit der i-Japan-Strategie 2015,¹¹ als Fortsetzung von „e-Japan“, „u-Japan“ und der „neuen IT-Reformstrategie“ ein nachfolgender Entwurf für die Zukunft der Informatisierung in Japan erstellt (Yao Guozhang & Lin Ping 2009). „Der Hauptschwerpunkt der „i-Japan-Strategie 2015“ liegt auf drei Bereichen der Digitalisierung, nämlich E-Regierung, medizinisches Gesundheitswesen und Personalbildung“ (Hai Qun & Urna 2010). Um die IT-Entwicklung zu fördern und den Menschen und der Gesellschaft den größtmöglichen Nutzen zu bringen, hat die japanische Regierung 2013 die Erklärung abgegeben, der weltweit fortschrittlichste IT-Nation-Grundplan zur Förderung der flexiblen Datennutzung von öffentlichen und privaten Bereichen, bei der eine flexible IT-Anwendung als Entwicklungsstrategie mit relevanter Infrastruktur unter Anleitung des Chefinformationsbeamten der Regierung verstärkt wurde. Für die olympischen und paraolympischen Spiele 2020 in Tokio wurden verschiedene politische Erleichterungsmaßnahmen eingeführt (Lian Cheng, Yang Fei & Zhang Hengye 2018).

11 Der Buchstabe „i“ in der „i-Japan-Strategie 2015“ hat zwei Bedeutungen: Inklusion und Innovation. Inklusion repräsentiert ursprünglich das „Beinhalten“, hier bedeutet, dass IKT wie Sonnenschein, Wasser und Luft in alle Aspekte der wirtschaftlichen und sozialen Entwicklung integriert werden sollen, während unter Innovation Kreativität und Innovationsgeist verstanden werden.

Tabelle 5-6 Strategien der digitalen Regierung der wichtigsten Länder

Land	Strategien der digitalen Regierung	Jahr	Hauptinhalt
Japan	i-Japan Strategie 2015	2009	Der Buchstabe „i“ in der „i-Japan-Strategie 2015“ hat zwei Bedeutungen: Inklusion und Innovation. Die vordere bedeutet, dass IKT wie Sonnenschein, Wasser und Luft in alle Aspekte der wirtschaftlichen und sozialen Entwicklung integriert werden sollen, während die hintere Kreativität und Innovationsgeist bedeutet. Der Hauptschwerpunkt der „i-Japan-Strategie 2015“ liegt im Digitalisierungsprozess der Bereich: nämlich E-Regierung, medizinisches Gesundheitswesen und Personalbildung.
Südkorea	Intelligenter Regierungsplan	2011	Ziel ist es, bis 2015 eine intelligente Regierung aufzubauen. Die Umsetzungsstrategie umfasst vier Aspekte: Offenheit, Integration, Koordination sowie nachhaltiges und grünes Wachstum.
Vereinigtes Königreich	Digitale Strategie der Regierung	2012	Die Strategie erläutert die aktuelle Situation, Hindernisse, Erfolge und künftige Aktionspläne für digitale Dienste im Vereinigten Königreich und leitet verschiedene Abteilungen eigene Digitalisierungsstrategien zu formulieren, um die Verbesserung und Entwicklung digitaler Dienste zu fördern. Ihr Kern besteht darin, die Bereitstellung digitaler Dienste als die bevorzugte Möglichkeit für die Regierung zu betrachten, öffentliche Dienste bereitzustellen. Ziel ist es, Bedingungen für Menschen zu schaffen, die sich für Nutzung digitaler Kanäle entscheiden, und Bedingungen für Menschen zu schaffen, die diese nicht nutzen können.

(Fortsetzung)

Tabelle 5-6 Fortsetzung

Land	Strategien der digitalen Regierung	Jahr	Hauptinhalt
Vereinigte Staaten	Digitale Regierung: Aufbau einer Plattform des 21. Jahrhunderts, um dem amerikanischen Volk besser zu dienen	2012	Ziel ist es, mehr Innovationen zu geringeren Kosten zu schaffen und es Unternehmen zu ermöglichen, Regierungsdaten besser zu nutzen, um die Qualität der für das amerikanische Volk erbrachten Dienstleistungen zu verbessern.
Singapur	Smart Nation 2025 Plan	2014	Um den Bürgern, der Regierung und den öffentlichen Diensten Singapurs zu helfen, auf beispiellose Weise miteinander verbunden zu werden, damit Institutionen und Bürger vom Zugang zu Daten profitieren können. „Smart Nation“ ist für Bürger, Unternehmen und ihre Partner von großer Bedeutung.
Frankreich	Aktionsplan zur Förderung des Aufbaus der Digitalen Republik	2015	Erstens fördert es die Datenwirtschaft, indem es das Konzept von Daten von universellem Interesse schafft. Zweitens sollen tatsächliche Allianzen für Open Innovation geschlossen werden, indem die Zusammenarbeit zwischen traditionellen und neugegründeten Unternehmen gefördert wird und drittens fördert es die offene Wissenschaft mit offenem Zugang zu Veröffentlichungen und Forschungsdaten.
Deutschland	Digitalisierungsstrategie 2025	2016	Es legt Ziele in Schlüsselbereichen der Entwicklung digitaler Regierungen dar und schlägt spezifische und zielgerichtete Umsetzungsmaßnahmen vor, die eine wichtige Rolle bei der Beschleunigung des Fortschritts in Richtung Industrie 4.0 in Deutschland spielen.

Tabelle 5-6 Fortsetzung

Land	Strategien der digitalen Regierung	Jahr	Hauptinhalt
Dänemark	Digitale Strategie 2016–2020	2016	Es ist eine Fortsetzung und Weiterentwicklung der digitalen Regierungsstrategie 2011–2015 und definiert den Digitalisierungsprozess im öffentlichen Sektor Dänemarks und dessen Interaktion mit Unternehmen und Branchen, um den Grundstein für ein starkes und sicheres digitales Dänemark zu legen.
Schweden	Digitale Strategie: Schwedens nachhaltige digitale Transformation	2017	Es umreißt die wichtigsten Punkte der Digitalisierungspolitik der Regierung und drückt Schwedens Vision einer nachhaltigen digitalen Transformation aus. Das Hauptziel ist es, Schweden zu einem weltweit Führer zu machen, der die Chancen der digitalen Transformation nutzt.
Australien	Strategie für die digitale Transformation der Regierung 2025	2018	Die Hauptaufgabe besteht darin, die Bereitstellung öffentlicher Dienste durch eine zentrale Datenbank zu verbessern, in der offene Regierungsdaten gespeichert und neue Werte für Benutzer und die gesamte Gesellschaft geschaffen werden. Die strategische Vision ist es, Australien bis 2025 zum Nutzen aller Australier zu einem der drei weltweit Führer für Entwicklung digitaler Regierungen zu machen.

Quelle: Siehe „Bericht über Entwicklung der digitalen Regierung 2019“, in E-Regierung-Forschungszentrum der Parteischule des Zentralkomitees der KP Chinas (Staatliche Verwaltungshochschule), 2019

Abschnitt II Chinas Datenrechtssystem

Der Schutz von Datenrechten ist zu einem wichtigen Thema geworden, das niemand in der heutigen Gesellschaft vermeiden kann. Die meisten Länder der Welt stärken den Schutz der Datenrechte durch innerstaatliche Gesetzgebung, um den Zweck des Schutzes der Rechte der Datenrechtsinhaber zu erreichen. An einem wichtigen Punkt der neuen Runde der technologischen Revolution und des industriellen Wandels hält China an den Chancen der digitalen, internetbasierten und intelligenten Entwicklung fest und reagiert aktiv auf die Herausforderungen, die sich aus der Entwicklung von Big Data in den Bereichen Recht, Sicherheit und Regierungsverwaltung usw. ergeben. In China nimmt das Rechtssystem zum Schutz der Datenrechte erst Gestalt an: vom Strafrecht, Zivilrecht bis zum Verwaltungsrecht, von Gesetzgebung des Nationalen Volkskongresses zu Abteilungs-vorschriften und Branchenstandards, von Datenteilhabe zu offenem Zugang zu Daten und von Datensicherheitsmanagement zur digitalen Regierungsverwaltung usw. all dies zusammen bildet ein Rechtssystem zum Schutz der Datenrechte mit klarer Eigenheit der „chinesischen Rechtsstaatlichkeit“.

(I) Gesetzssystem für Schutz der Datenrechte

Auf der nationalen Ebene sind die Bestimmungen zum Schutz der Datenrechte hauptsächlich in verschiedenen Rechtsbereichen wie der Verfassung, dem Strafrecht, dem Zivilrecht und anderen Gesetzen verteilt (siehe Tabelle 5-7). Derzeit enthält jedoch kein Gesetz oder keine Vorschrift zum Schutz von Datenrechten eine praktikable Definition von Datenrechten und es gibt auch keinen klaren Umfang der Datenrechte, die geschützt werden sollen. Man kann auch Mängel an systematischer Struktur, Konsistenz und Folgerichtigkeit sowie anderen Einschränkungen in Bezug auf den Schutzzumfang und vager Anwendbarkeit der Schutzstandards feststellen.

I. Verfassungsschutz

Die Bestimmungen der Verfassung sind Grundlage für den Schutz des Rechts auf personenbezogene Daten und Informationen. Die Klausel über die „Persönlichkeitswürde“ in Artikel 38 der Verfassung bietet Raum für Auslegung neuer Grundrechte in Bezug auf die Persönlichkeit, einschließlich des Schutzes der Rechte auf persönlichen Informationen und Daten. Die Klausel „Der Staat achtet und wahrt Menschenrechte“ in Artikel 33 der Verfassung wird als allgemeine Rechtsklausel in der Verfassung Chinas angesehen. Sie ist auch die Hauptgrundlage für das Bestehen der Rechte auf Informationen und Daten als Grundrecht, das nicht ausdrücklich aufgeführt ist. Weitere relevante Klauseln sind Artikel 37 über die Unantastbarkeit der persönlichen Freiheit, Artikel 39 über die Unverletzlichkeit der Wohnungen, Artikel 40 über den gesetzlichen Schutz der Freiheit und der Privatsphäre der Korrespondenz sowie Artikel 41 über das Recht, Kritik zu üben und Vorschläge zu machen, Beschwerden, Klagen oder Anzeigen zu erheben usw. Diese spezifischen Bestimmungen zu Grundrechten sind direkt oder indirekt mit dem Recht auf Schutz von Informationen und Daten verbunden, während die Verwirklichung dieser konkreten Grundrechte eine starke Garantie für Verwirklichung des Rechts auf Informationsselbstbestimmung bietet. Das Recht auf Schutz von Informationen und Daten ist im Wesentlichen Teil des Kerninhalts der Grundrechte, nämlich der Menschenwürde und der Unabhängigkeit der Persönlichkeit. Der Schutz von Informationen und Daten ist ein Muss der Sozialdemokratie, die Voraussetzung der Autonomie der Bürger und die starke Garantie für Verwirklichung der individuellen Freiheit in einer demokratischen Gesellschaft. Gleichzeitig ist es auch das unvermeidliche Ergebnis der Anpassung des Grundrechtssystems an die Entwicklung der Informationsgesellschaft (Li Aijun 2018, S. 24).

2. Strafrechtlicher Schutz

Die Handlung der Verletzung des Rechts der Bürger auf personenbezogene Daten liegt weit außerhalb der Kontrolle durch das Zivilrecht und Verwaltungsrecht. Die 2009 und 2015 verabschiedeten Änderungsanträge

VII und IX des Strafrechts enthalten entsprechende Bestimmungen zu Straftaten im Zusammenhang mit personenbezogenen Informationen und Daten. Artikel 253 des überarbeiteten Strafrechts IIV enthält das neu hinzugefügte Verbrechen, persönliche Informationen der Bürger zu verkaufen oder illegal zu liefern und persönliche Informationen von Bürger illegal zu erhalten. Durch Änderung IX des Strafrechts wurden die Bestimmungen zur Sicherheit personenbezogener Daten in großem Maße überarbeitet und vervollständigt. Zunächst wurde Artikel 253A teilweise geändert, wobei das Verbrechen des Verkaufs und der illegalen Lieferung persönlicher Informationen sowie des illegalen Erhaltens persönlicher Informationen von Bürgern beseitigt und das Verbrechen der Verletzung persönlicher Informationen von Bürgern hinzugefügt wurde.¹² Dies stellt insbesondere eine Erweiterung des Umfangs möglicher Täter auf der Grundlage von Änderungsantrag VII des Strafrechts dar, deren Umfang über das Personal staatlicher Organe oder von Finanz-, Telekommunikations-, Transport-, Bildungs-, medizinischen und anderen Institutionen hinausgeht und die Strafen für die oben genannten Fälle von erwähntem Personal, das das Verbrechen begeht, die persönlichen Daten der Bürger zu verletzen, werden erhöht. Darüber hinaus wird in Artikel 286 das Verbrechen der Nichterfüllung der Verpflichtung zum Sicherheitsmanagement des Informationsnetzwerks und in Artikel 287 das Verbrechen der illegalen Nutzung des Informationsnetzwerks und der Unterstützung krimineller Aktivitäten über ein Informationsnetz hinzugefügt (Yao Yuerong 2011, S. 22–23), die das Datenrecht der Bürger klar spezifiziert und nachdrücklich schützt. Im Zeitalter von Big Data ist es unbedingt erforderlich, den Schutz personenbezogener Daten aus strafrechtlicher Sicht zu stärken. Die diesbezüglichen Bemühungen zeigen Chinas Engagement für die Respektierung der Menschenrechte und den Schutz personenbezogener Daten der Bürger und haben wichtige Bedeutung.

12 Siehe die vom höchsten Volksgericht und der obersten Volksanwaltschaft am 30. 10. 2015 erlassene ergänzende Bestimmung (VI) zur Durchführung der Festlegung der Straftat des „Strafrechts der Volksrepublik China“ – rechtliche Darlegung Nr. 20/(2015).

3. Zivilrechtlicher Schutz

Im Jahr 2010 wurde das „Deliktsgesetz“ zur Durchführung verkündet und das „Recht auf Privatsphäre“ wurde erstmals als Bürgerrecht und -interesse eingeführt. Artikel 36, eine Bestimmung zur „Haftung für Netzwerkverletzung“, geht vom bisherigen indirekten Schutz des Rechts der Bürger auf Privatsphäre im Cyberspace weiter und präzisiert die rechtliche Haftung von Internetnutzern und Internetdiensteanbietern für Verletzungen des Rechts anderer Personen auf Privatsphäre. Das neu überarbeitete „Gesetz zum Schutz der Verbraucherrechte und -interessen“ von 2014 ist das erste spezialisierte Gesetz in China, das personenbezogene Daten mit detaillierten Bestimmungen schützt. Die Artikel 14, 29 und 50 sehen jeweils „das Recht auf gesetzmäßigen Schutz personenbezogener Daten“, „die Grundsätze und Pflichten, denen die Betreiber bei der Erhebung personenbezogener Daten folgen müssen“ und „die Rechtsbehelf der Beteiligten“ vor, die die direkten und spezifischen Bestimmungen zum Schutz der persönlichen Daten der Verbraucher sind. Die im März 2017 verabschiedeten „allgemeinen Bestimmungen des Zivilrechts“ haben das Recht auf „privaten Daten natürlicher Personen“ erstmals als Bürgerrecht angenommen. Artikel 110 sieht vor, dass eine natürliche Person das Recht auf Namen, Porträt, Ansehen und Ehre sowie das Recht auf Privatsphäre genießt. Artikel 111 sieht vor, dass personenbezogene Daten einer natürlichen Person gesetzlich zu schützen sind. Jede Organisation oder Einzelperson, die personenbezogene Daten anderer Personen zu erhalten braucht, muss diese Informationen rechtmäßig erhalten und deren Sicherheit gewährleisten, wobei sie die personenbezogenen Daten anderer Personen nicht illegal sammeln, verwenden, verarbeiten oder übermitteln oder illegal kaufen, verkaufen, liefern oder die persönlichen Daten anderer Personen nicht veröffentlichen darf“. Artikel 127 reagiert unmittelbar auf den rechtlichen Status von Daten, indem er vorsieht, dass „dieses Gesetz gilt, wenn ein Gesetz den Schutz von Daten und virtuellem Netzwerkvermögen vorsieht“. Dieser Schritt markiert die formelle Eingabe von Dateninformationen in den Geltungsbereich der zivilrechtlichen Regulierung und des zivilrechtlichen Schutzes und unterstreicht die Tatsache, dass die „allgemeinen Bestimmungen des Zivilrechts“ mit der Zeit Schritt halten.

4. Sonstiger rechtlicher Schutz

Der Schutz der Datenrechte ist ein kompliziertes und systematisches Projekt, das sich nicht nur auf die Verfassung, das Strafrecht und das Zivilrecht bezieht, sondern auch Anpassungen vieler anderer Gesetze betrifft. Es gibt also drei Kategorien davon. Die Erste ist der allgemein geltende gesetzliche Schutz, wie er durch das „Passgesetz“, das „Statistikgesetz“, das „Gesetz zur Wahrung der Staatsgeheimnisse“, das „Gesetz über den Personalausweis der Einwohner“ und das „nationale Sicherheitsgesetz“ usw. vorgesehen wird. Diese Gesetze sind normalerweise allgemeine Bestimmungen von Richtlinien, Rahmenbedingungen und Grundsätze für den Schutz personenbezogener Daten. Die zweite Kategorie zielt auf Schutz personenbezogener Daten bestimmter Bevölkerungsgruppen ab. Beispiele hierfür sind das „Gesetz zum Schutz Minderjähriger“ und das „Gesetz zum Schutz der Rechte und Interessen von Frauen“ usw., die durch den Schutz der personenbezogenen Daten bestimmter Bevölkerungsgruppen ihre Persönlichkeit, Würde und Freiheit vor Verletzung schützen und Wahrung ihrer legitimen Rechte und Interessen betonen. Das Ziel der dritten Kategorie liegt im Schutz personenbezogener Daten in bestimmten Bereichen. Beispiele sind das „Gesetz über praktizierende Ärzte“, das „Anwaltsgesetz“, das „Gesetz zur Prävention und Behandlung von Infektionskrankheiten“, das „Postgesetz“, das „Gesetz über Kommerzbanken“, das „Cybersicherheitsgesetz“, das „Gesetz über elektronische Signatur“ und das „Chiffre-gesetz“ etc. Diese Kategorie hat die größte „Anzahl“ von Gesetzen und auch die größte Abdeckung in Bezug auf Bereiche und Branchen. Die Bestimmungen dieser Gesetze sind hoch professionell, durchsetzbar und bedienbar und spielen eine unersetzliche Rolle im Rechtssystem zum Schutz der Datenrechte in China. Man kann sagen, dass diese drei Kategorien von Gesetzen entsprechende Bestimmungen für Schutz der Datenrechte auf verschiedenen Ebenen haben, die die legitimen Rechte und Interessen von Bürgern, juristischen Personen und anderen Organisationen wirksam schützen und zur Förderung einer gesunden und ordnungsmäßigen Entwicklung der Wirtschaft und Gesellschaft beitragen.

Tabelle 5-7 Gesetzliche Bestimmungen zum Schutz von Datenrechten in China

Kategorie	Bezeichnung des Rechts	Datum der Implementierung	Relevante Bestimmungen
Verfassung	Verfassung	11. März 2018	Artikel 33, 37, 38, 39, 41
Strafrecht	Strafrecht	4. November 2017	Artikel 253 (1), 286, 286 (1), 287, 287 (1), 287 (2)
Zivilrecht	Deliktsrecht	1. Juli 2010	Artikel 2, 36
	Gesetz zum Schutz der Verbraucherrechte und -interessen	15. März 2014	Artikel 14, 29, 50
	Allgemeine Bestimmungen des Zivilrechts	1. Oktober 2017	Artikel 110, 111, 127
Andere Gesetze	Passgesetz	1. Januar 2007	Artikel 12, 20
	Gesetz über praktizierende Ärzte	27. August 2009	Artikel 22, 37
	Statistikgesetz	1. Januar 2010	Artikel 9, 25, 37, 39
	Gesetz zur Bewachung von Staatsgeheimnissen	1. Oktober 2010	Artikel 23, 24, 25, 26
	Gesetz über den Personalausweis der Einwohner	1. Januar 2012	Artikel 6, 13, 19, 20
	Gesetz zur Prävention und Behandlung von Infektionskrankheiten	29. Juni 2013	Artikel 12, 68, 69
	Postrecht	24. April 2015	Artikel 7, 35, 36, 76
	Nationales Sicherheitsgesetz	1. Juli 2015	Artikel 51, 52, 53, 54
	Gesetz über Kommerzbanken	1. Oktober 2015	Artikel 6, 29

(Fortsetzung)

Tabelle 5-7 Fortsetzung

Kategorie	Bezeichnung des Rechts	Datum der Implementierung	Relevante Bestimmungen
	Cybersicherheitsgesetz	1. Juni 2017	Artikel 10, 18, 21, 22, 27, 37, 40, 41, 42, 43, 44, 45, 66, 76
	Anwaltsrecht	1. Januar 2018	Artikel 38, 48
	Gesetz über elektronische Signatur	23. April 2019	Artikel 15, 27, 34
	Cheffrier-Gesetz	1. Januar 2020	Artikel 1, 2, 7, 8, 12, 14, 17, 30, 31, 32

(II) Gesetzgebungspraxis in Bezug auf Datensicherheit

Ohne Datensicherheit könnte es keine staatliche Sicherheit geben. Die Gesetzgebung spielt eine grundlegende Rolle bei unseren Bemühungen um die Gewährleistung der Datensicherheit. Nur auf dem Weg zur Rechtsstaatlichkeit können wir ein Gleichgewicht zwischen der Anwendung und Sicherheit von Big Data erreichen und die Sicherheit für den Staat, die öffentlichen Interessen und Einzelpersonen gewährleisten, während Big Data optimal genutzt wird. Gegenwärtig bemüht sich China, die Chance der Entwicklung von Big Data zu nutzen und aktive Versuche zur Gesetzgebung zur Datensicherheit zu unternehmen. In diesem Bereich wurde ein Soundsystem geschaffen, bei dem der „Staat die Sache vorantreibt, die lokalen Behörden als Pioniere fungieren und Experten daran appellieren“.

1. Nationale Gesetzgebungspraktiken

Im Zeitalter von Big Data hat die Datensicherheit nicht nur einen großen Einfluss auf die gesunde Entwicklung der Big-Data-Branche, sondern kann auch eine ernsthafte Bedrohung für die staatliche Sicherheit darstellen. Daher ist die Datensicherheit eines der dringendsten Probleme,

die wir im Bereich der Informationssicherheit im Zeitalter von Big Data angehen müssen. Gemäß dem vom Staatsrat am 5. September 2015 herausgegebenen „Aktionsprogramm zur Förderung der Entwicklung von Big Data“ sollen die Rechts- und Standardsysteme verbessert werden, um Big Data auf wissenschaftliche und standardisierte Weise zu nutzen und die Datensicherheit wirksam zu schützen. Am 8. Dezember 2017 wies Präsident Xi Jinping während der zweiten kollektiven Studiensitzung zur Umsetzung der Nationalen Big-Data-Strategie des Politbüros des CPC-Zentralkomitees darauf hin, dass „Anstrengungen unternommen werden sollen, um die nationale Datensicherheit wirksam zu gewährleisten. Wir sollen den Sicherheitsschutz der Schlüsselinformationsinfrastruktur stärken, unsere Kapazitäten zum Schutz der Schlüsseldatenressourcen ausbauen und unsere Fähigkeit zur Frühwarnung und Rückverfolgung der Datensicherheit verbessern. Die Koordinierung zwischen Politik, Aufsicht und Gesetzen soll verbessert und der Aufbau von Rechtssystemen beschleunigt werden. Es sollen Systeme für die Bestätigung, den offenen Zugang, die Verbreitung und den Handel von Datenressourcen eingerichtet und das System zum Schutz der Rechte an Dateneigentum verbessert werden“. Dies erfordert, dass wir uns an den ganzheitlichen Ansatz der staatlichen Sicherheit halten, eine angemessene Haltung gegenüber der Cybersicherheit einnehmen, Sicherheit und Entwicklung gleichermaßen Bedeutung beimessen, den Aufbau unseres Big-Data-Sicherheitssystems beschleunigen und eine reibungslose Umsetzung unserer nationalen Big-Data-Strategie sicherstellen.

Das „Cybersicherheitsgesetz“ ist ein wirksames gesetzliches Instrument für China, um die Sicherheitsherausforderungen im internationalen Cyberspace zu bewältigen, unsere Souveränität im Cyberspace zu wahren und die legitimen Rechte und Interessen der Bürger im Cyberspace vor der Verletzung zu schützen. Als das erste Gesetz auf dem Gebiet der Cybersicherheit in China enthält das „Cybersicherheitsgesetz“ klare Bestimmungen zur Datensicherheit, Informationssicherheit im Cyberspace usw., die eine rechtliche Grundlage für die Förderung der Datennutzung, Garantie der Datensicherheit und Wahrung der nationalen Datensouveränität bilden. Gemäß Artikel 21 des „Cybersicherheitsgesetzes“ müssen Netzbetreiber Maßnahmen wie die Klassifizierung, Sicherung und Verschlüsselung

wichtiger Daten ergreifen, um Verstohlenheit oder Manipulationen der Cyberdaten zu verhindern. In den Artikeln 37 und 38 ist festgelegt, dass die Betreiber kritischer Informationsinfrastrukturen wichtige Daten wie die personenbezogenen Daten im Hoheitsgebiet der Volksrepublik China speichern, wenn es tatsächlich erforderlich ist, solche Daten im Ausland gespeichert oder nach dem Ausland abgeliefert zu werden, soll Sicherheitsbewertung gemäß entsprechenden Bestimmungen durchgeführt werden. Die Artikel 40 bis 45 sehen vor, dass die Netzbetreiber die von ihnen gesammelten personenbezogenen Benutzerdaten streng geheim halten und ein System zum Schutz der Benutzerinformationen einrichten und verbessern. Sie dürfen keine personenbezogenen Daten anderer Personen rechtswidrig oder vertragsbrüchig sammeln, verwenden oder verarbeiten, um zu verhindern, dass personenbezogene Daten und Informationen der Bürger illegal abgerufen, durchgesickert oder illegal verwendet werden. Artikel 47 legt ausdrücklich die Verpflichtung der Netzbetreiber in Bezug auf die Verfügung über illegale Informationen fest: Wenn ein Betreiber Informationen findet, deren Freigabe oder Übertragung durch ein Gesetz oder eine Verwaltungsvorschrift verboten ist, soll er die Übertragung dieser Informationen unverzüglich einstellen, diese löschen oder jede andere Handhabungsmaßnahme treffen, um die Verbreitung der Informationen zu verhindern, relevante Aufzeichnungen aufzubewahren und sie der zuständigen Behörde zu melden (Li Aijun 2018, S. 27). Man kann sagen, dass das „Cybersicherheitsgesetz“ Raum für Entwicklung der Datenzirkulation und -transaktion in China gelassen hat und auch eine starke Garantie für den Schutz personenbezogener Daten bietet.

Kryptogramme sind eine wichtige nationale strategische Ressource mit direktem Einfluss auf die nationale Datensicherheit. Am 26. Oktober 2019 wurde das chinesische „Chiffriergesetz“ offiziell verkündet, wodurch die Kryptographie als Kerntechnologie für die Datensicherheit in China etabliert und in eine zentrale Position im Bereich der Datensicherheit gebracht wurde. Mit 44 Artikeln in fünf Kapiteln enthält das „Chiffriergesetz“ klare Bestimmungen zum Führungs- und Managementsystem für Kryptographie, zu den Grundsätzen für das klassifizierte Management von Kryptographie, zur szenenbasierten Anwendung von Kryptographie sowie zur Förderung und Unterstützung der Entwicklung der Kryptographie. Das

„Chiffriergesetz“ ist mit dem „Cybersicherheitsgesetz“, dem „Gesetz zum Schutz staatlicher Geheimnisse“ und anderen damit zusammenhängenden Gesetzen und Vorschriften gut verbunden. Es hat auch den kryptographischen Grundstein für das nachfolgende „Datensicherheitsgesetz“ und das „Gesetz zum Schutz personenbezogener Daten“ gelegt. Als das erste Gesetz auf dem Gebiet der Kryptographie in China bietet das „Chiffriergesetz“ eine solide Rechtsgrundlage für den verschlüsselten Datenschutz und beendet damit die Zeit, in der „Daten im ganzen Internet ungeschützt bleiben“ und in großem Umfang missbraucht werden. Da alle Arten von kryptografischen Anwendungen für die Datenverschlüsselung und den Datenschutz in größerem Umfang eingesetzt werden, wird das Internet in China sicherer und kontrollierbarer. Dies wird einen starken Impuls für die gesunde und nachhaltige Entwicklung des Internets in China geben und eine große Hilfe für unsere Bemühungen zur Stärkung und Förderung des Schutzes der Datensicherheit in unserem Land darstellen.

Am 28. Mai 2019 wurden die „Maßnahmen zur Verwaltung der Datensicherheit“ (Entwurf zur Stellungnahme) (im Folgenden kurz als „Maßnahmen“ genannt) offiziell veröffentlicht. Diese „Maßnahmen“ wurden in Übereinstimmung mit dem „Cybersicherheitsgesetz“ und anderen relevanten Gesetzen und Vorschriften formuliert. Inhaltlich haben diese „Maßnahmen“ vor allem Anpassungen in Bezug auf das Sicherheitsmanagement und den Schutz wichtiger Daten und personenbezogener Daten vorgenommen und entsprechende Standards für Erhebung, Verarbeitung und Verwendung personenbezogener Informationen und wichtiger Daten sowie die einschlägige Sicherheitsüberwachung und -verwaltung abgeklärt und den Vorschlag gemacht, dass Netzbetreiber, die wichtige Daten oder sensible personenbezogene Informationen zum Zweck des Betriebs sammeln, sich bei den örtlichen Cyberspace- und Informationsbehörden registrieren lassen sollen und Netzbetreiber, die personenbezogene Daten über Websites, Anwendungen und andere Produkte sammeln und verwenden, separate Regeln für die Erfassung und Verwendung formulieren sollen. 2018 führte die Europäische Union die „Allgemeine Datenschutzverordnung“ ein, die als das strengste Datenschutzgesetz in der Geschichte gilt. Es hat nicht nur den Schutz der Rechte auf personenbezogenen Daten ausführlich beschrieben, sondern auch schwerwiegende Strafmaßnahmen

gegen verstoßende Handlungen festgelegt. Nachdem die oben genannten „Maßnahmen“ in China erlassen worden waren, hielten einige Praktiker sie für noch strenger als die der EU. Darüber hinaus wurde das „Datensicherheitsgesetz“ im September 2018 offiziell in die Legislativagenda des Ständigen Ausschusses des 13. Nationalen Volkskongresses aufgenommen und die Gesetzgebung zur Datensicherheit wurde zu einer nationalen Strategie. Am 4. März 2019 sagte der Sprecher Zhang Yesui auf der Pressekonzferenz der zweiten Sitzung des 13. Nationalen Volkskongresses, dass die Arbeit an der Umsetzung des „Datensicherheitsgesetzes“ im Jahr 2019 vorangetrieben werde, um die Fähigkeit für Prävention und Widerstand gegen Sicherheitsrisiken zu erhöhen.

2. Legislative Versuche auf lokaler Ebene

Die Lokale Gesetzgebung hat die einzigartigen Vorteile von hoher Flexibilität, niedrigen Kosten für Probefehler und klaren Besonderheiten. Sie bietet nicht nur eine starke institutionelle Garantie für die Erforschung innovativer Experimente und die Förderung der sozialen Entwicklung innerhalb der Region, sondern sammeln auch viele wertvolle Erfahrungen, mit denen wir den „Weg zur Regierungsführung Chinas“ ebnen können. Dies ist von äußerst wichtigem Wert und spielt eine unersetzliche positive Rolle bei der vollständigen Umsetzung der nationalen Grundstrategie der Rechtsstaatlichkeit. Datensicherheit ist die Voraussetzung für die Entwicklung und Anwendung von Big Data. Ohne Datensicherheit wird die Entwicklung und Anwendung von Big Data nicht nachhaltig sein und die Big-Data-Branche kann sich nicht auf gesunde Weise entwickeln. Die Provinz Guizhou und die Stadt Tianjin sind Vorreiter und führende Kräfte bei der Gesetzgebung zu Big Data auf lokaler Ebene. Sie sind auch als Hauptschlachtfeld der nationalen zusammenfassenden Big-Data-Pilotzonen ausgewiesen. Bis November 2019 haben diese beiden Orte sechs lokale Gesetze und Vorschriften für Big Data formuliert, fünf von Guizhou und eines von Tianjin. Solche lokalen Gesetzgebungsbemühungen haben wissenschaftliche Leitlinien und gesetzliche Unterstützung für Entwicklung der Big-Data-Industrie in Tianjin und Guizhou geliefert, insbesondere für das Management

der Datensicherheit. Andere Orte wie Shanghai, Chongqing, Zhejiang und Fujian usw. haben ebenfalls Regierungsverordnungen formuliert, um das Datensicherheitsmanagement, die Datenoffenheit und Teilhabe an Daten und Datenanwendung und Datendienste zu verbessern (siehe Tabelle 5-8). Diese Gesetzgebungspraktiken auf lokaler Ebene in Bezug auf Datenrechte haben einige Beiträge zur Regelung der Verwaltung der Erhebung, Verwendung und Verarbeitung von Daten sowie zur Wahrung der Datensicherheit und zum Schutz der legitimen Rechte und Interessen der Datenrechtsinhaber geleistet.

Guizhou gehört zu den ersten Provinzen in China, die die Big-Data-Branche am frühesten entwickelt haben. 2013 war das Jahr der Planung für Entwicklung der Big Data und konkrete Programme wurden 2014 offiziell gestartet. Die Provinz Guizhou positionierte sich erfolgreich als einer der „Vorreiter“ in der Big-Data-Entwicklung und stand Schulter an Schulter mit Guangdong, Peking und Tianjin. Im Januar 2016 führte die Provinz Guizhou Chinas erste lokale Verordnung zu Big Data, die „Verordnung der Provinz Guizhou zur Förderung der Entwicklung und Anwendung von Big Data“ ein, mit Grundsätzen, allgemeinen Bestimmungen und Richtlinien für das Management der Sicherheit von Big Data (Artikel 4, 29, 31, 32 und 33). „Inmitten der rasanten Entwicklung sind Probleme mit der Sicherheit von Big Data immer offensichtlicher geworden: Erstens gibt es eine große Anzahl von Sicherheitsrisiken für Big Data. Zweitens wird der Konflikt zwischen den Anforderungen an Sicherheit von Big Data und der Nachfrage nach Offenheit und Teilhabe immer markanter. Drittens sollen die Gesetze und Vorschriften zur Sicherheit von Big Data noch verbessert werden“ (Kommission für Legislative Angelegenheiten des Ständigen Ausschusses des Volkskongresses der Provinz Guizhou 2019, S. 4). Daher wurde auf der Legislativarbeitssitzung des Ständigen Ausschusses des 13. Volkskongresses der Provinz Guizhou ausdrücklich darauf hingewiesen, dass „wir uns dringend Zeit nehmen sollen, um lokale Gesetze und Vorschriften zur Sicherheit von Big Data in der Provinz Guizhou zu studieren und einzuführen“. Im August 2019 war die Provinz Guizhou erneut Vorreiter bei der Einführung von Chinas erster Big-Data-Sicherheitsverordnung in der Provinz, den „Verordnungen zur Gewährleistung der Big-Data-Sicherheit der Provinz Guizhou“ (im Folgenden kurz als „Verordnungen“

genannt). Auf der Grundlage der „Bestimmungen zur Entwicklung und Anwendung der Big Data der Provinz Guizhou“ haben die „Verordnungen“ entsprechende Aspekte der Garantie der Big-Data-Sicherheit verfeinert, Verantwortlichkeiten für die Big-Data-Sicherheit, Überwachung und Verwaltung sowie rechtliche Verpflichtungen der für die Big-Data-Sicherheit Verantwortungsträger klar definiert und das Konzept verkörpert, Entwicklung und Sicherheit gleichermaßen zu berücksichtigen und Entwicklung durch Sicherheit und Förderung der Sicherheit durch Entwicklung zu gewährleisten. Die „Verordnungen“ zielen darauf ab, „acht Systeme“¹³ für den Schutz der Big-Data-Sicherheit zu schaffen, wobei der Schwerpunkt auf der Verbesserung der umfassenden Verteidigungs- und Verwaltungsfähigkeiten für die Big-Data-Sicherheit in der gesamten Gesellschaft liegt und auf drei Kernprobleme der Entwicklung der Big-Data-Branche reagiert: „Erstens hat man sich dem Problem der Priorisierung der Entwicklung der Big-Data-Branche gegenüber Vernachlässigung des Schutzes der Sicherheit in der vorherigen Entwicklung gestellt und spezielle Gesetze zum Schutz der Sicherheit von Big Data eingeführt; zweitens hat man als Reaktion auf das Problem ‚mehrerer Regulierungsbehörden aber ohne klare Arbeitsteilung‘ im Prozess der Entwicklung und Anwendung von Big Data klargestellt, wer für die Sicherheit von Big Data zuständig ist und ihre spezifischen Verantwortlichkeiten sind definiert; drittens hat man die Beziehungen zwischen Öffnung zur Teilhabe und Sicherheit deutlich gemacht“ (He Xinghui 2019). Die Umsetzung der „Verordnungen“ ist von großer Bedeutung für Gewährleistung der Sicherheit von Big Data und persönlichen Informationen sowie für Klärung der Verantwortlichkeiten für die Sicherheit von Big Data und die Förderung der Entwicklung und Anwendung von Big Data. Sie legen auch eine solide theoretische und praktische Grundlage für die Gesetzgebung zur Sicherheit von Big Data und zum Schutz personenbezogener Daten auf nationaler Ebene.

13 Die acht große Systeme zum Schutz der Big-Data-Sicherheit sind das Organisationssystem, das Präventionssystem, das Überwachungs- und Regulierungssystem, das Notfallreaktionssystem, das umfassende Schutzsystem, das technische Service-System, das System zur Personalaus- und -weiterbildung und das Arbeitsunterstützungssystem für die Big-Data-Sicherheit.

Guiyang hat als Kernbereich der umfassenden Pilotzone von National Big Data (Guizhou) stets großen Wert auf „Systeminnovationen“ gelegt, um die wichtige strategische Schlüsselaufgabe beim Aufbau des „China Data Valley“ zu erfüllen. Dazu wurde der Vorschlag für das Top-Level-Design „1 + 1 + 3 + N“¹⁴ für die Entwicklung der Big-Data-Sicherheit gemacht und Guizhou verpflichtete sich zum Aufbau einer nationalen Pilot- und Demonstrationszone für Big-Data- und Cyber-Sicherheit. Im Mai 2017 wurde Guiyang offiziell vom Ministerium für öffentliche Sicherheit genehmigt, die erste „Pilotstadt des Landes für Demonstration von Big-Data- und Cyber-Sicherheit“ aufzubauen. Dies war ein Zeichen für den Beginn der neuen Bemühungen der Stadt Guiyang im Bereich der Big-Data-Sicherheit, ein neues Stadtmodell für Big-Data-Sicherheit zu schaffen. Im Jahr 2018 hat Guiyang die „Bestimmungen zum Big-Data-Sicherheitsmanagement“ in Übereinstimmung mit den Bestimmungen des „Cyber-Sicherheitsgesetzes“ und anderen relevanten Gesetzen und Bestimmungen in Verbindung mit der Arbeitspraxis zusammengestellt. Diese Verordnungen wurden am 1. Oktober 2018 in Kraft gesetzt. In den sechs Kapiteln sind 37 Artikel enthalten, einschließlich Allgemeine Bestimmungen, Sicherheitsgarantie; Überwachung, Frühwarnung und Notfallreaktion; Überwachung und Inspektion sowie rechtliche Verbindlichkeiten und ergänzende Bestimmungen. In Bezug auf die Sicherheitsgewährleistung heißt es in den Verordnungen eindeutig: „Der gesetzliche Vertreter oder der Hauptverantwortliche für ein Unternehmen

14 In 1 + 1 + 3 + N zeigt die erste „1“ die Realisierung der Guiyangs Absicht an, eine Pilotstadt für Demonstration von Big-Data- und Cybersicherheit zu werden und ist schon zu treibender Kraft für Entwicklung von Big-Data-Sicherheit geworden. Die zweite „1“ steht für den Plan, in Guiyang einen Schießstand für Big-Data-Sicherheit zu errichten, der sowohl für gewerbliche als auch für zivile Zwecke im Bereich der künftigen Internetsicherheit und Big-Data-Sicherheit geeignet ist und Zertifizierung und Sicherheitsüberprüfung für verschiedene Produkte, Technologien und Dienstleistungen bietet; die „3“ zeigt Guiyangs Absicht an, das „Situationsbewusstseinszentrum für städtische Sicherheit“, das „Überwachungszentrum für städtische Sicherheit“ und das „Innovationszentrum für Big-Data-Sicherheit“ zu errichten. Und das „N“ bezieht sich auf die verschiedenen Plattformen, die für Datensicherheit und Cybersicherheit in verschiedenen Bereichen und Branchen gebaut werden sollen.

mit Sicherheitsverantwortung ist die erste verantwortliche Person für die Sicherheit von Big Data in diesem Unternehmen. Ein Unternehmen mit Sicherheitsverantwortung muss Richtlinien für vollkommene Maßnahmen für Zugriffskontrolle formulieren und verbessern, technische Maßnahmen wie autorisierten Zugriff und Identitätsauthentifizierung usw. ergreifen, um unbefugte Abfragen, Replikation, Änderung und Übertragung von Daten zu verhindern. Personenbezogene Informationen und wichtige Daten werden durch Verschlüsselung und andere Sicherheitsmaßnahmen geschützt, und Daten, die sich auf die Sicherheit des Staates, soziale und öffentliche Interessen, Geschäftsgeheimnisse und personenbezogene Informationen beziehen, werden gesetzmäßig entschlüsselt und maskiert (Tageszeitung Guiyang 2018). Als erste lokale Vorschriften für das Big-Data-Sicherheitsmanagement in China verfeinern die Verordnungen nicht nur die Verantwortlichkeiten der Regierung und der zuständigen Behörden auf institutioneller Ebene gemäß dem Cybersicherheitsgesetz, sondern realisieren auch die Echtzeit- und dynamische Allwetter-Überwachung der Sicherheitsrisiken für wichtige Big Data, die für die Entwicklung der Big-Data-Industrie und Entwicklung der Rechtsstaatlichkeit in Bezug auf die Big-Data-Sicherheit in China von großer Bedeutung sind. Darüber hinaus haben Artikel 24 und 25 der „Bestimmungen über Öffnung und Teilhabe an Daten der Stadtregierung Guiyang“ (2017), Artikel 26 der „Verordnungen über Anwendung und Entwicklung von Gesundheits- und medizinischen Big Data der Stadt Guiyang“ (2018) sowie Artikel 46 bis 51 der „Bestimmungen zur Förderung der Entwicklung und Anwendung von Big Data der Stadt Tianjin (2018) klare Vorschriften zum Datensicherheitsmanagement festgelegt. Die Formulierung und Umsetzung dieser lokalen gesetzlichen Vorschriften ist von großer Bedeutung, um das Bewusstsein für Datensicherheit in der ganzen Gesellschaft zu stärken, die Fähigkeit zum Schutz der Datensicherheit in der gesamten Gesellschaft zu steigern und die Schaffung eines soliden rechtstaatlichen Umfelds zu fördern, in dem „jeder für die Datensicherheit verantwortlich“ ist. Sie haben eine nützliche Referenz für Formulierung von Gesetzen und Vorschriften zur Datensicherheit auf nationaler Ebene geliefert und regionale Weisheit gewidmet.

3. Empfehlungen von Experten für Gesetzgebung

Da die Bedingungen für Gesetzgebung zur Datensicherheit auf nationaler Ebene allmählich ausgereift sind, kommen immer lautere Stimmen aus allen Sozialbereichen, die die Gesetzgebung zur Datensicherheit anfordern. Während der „zwei Konferenzen“ (jährlichen Treffen des Nationalen Volkskongresses (NPC) und der Politischen Konsultativkonferenz des Chinesischen Volkes (CPPCC)) in den letzten Jahren haben viele Teilnehmer nachdrücklich die Einführung des Datenschutzgesetzes auf nationaler Ebene eindringlich appelliert. Zum Beispiel sagte der NPC-Abgeordnete Zheng Jie, dass bei der Datensicherheit um die Cybersicherheit, die Staatssicherheit, die Rechte und Interessen der Bürger auf Privatsphäre sowie um die soziale Sicherheit und Stabilität geht, weshalb die Formulierung eines Datensicherheitsgesetzes beschleunigt werden sollte. Er schlug vor: „Wir sollten die Datenhoheit begründen, den Geltungsbereich des Datensicherheitsgesetzes klar definieren und klarstellen, dass personenbezogene Informationen und wichtige Daten, die im Rahmen von Operationen innerhalb des Landes gesammelt und generiert werden, im Hoheitsgebiet der Volksrepublik China gespeichert werden sollen; ein Sicherheitsbewertungsmechanismus für den Datenausgang soll vervollständigt werden; der Anwendungsbereich dieses Mechanismus soll von den im Cybersicherheitsgesetz vorgesehenen wichtigen Betreibern der Informationsinfrastrukturen auf andere Netzbetreiber ausgeweitet werden und datenbezogene Aktivitäten, die für Interessen des Staates, der Unternehmen, Organisationen und Bürger relevant sind, sollen in den Geltungsbereich des Datensicherheitsgesetzes einbezogen werden“ (Zhao Yingying 2019).

Das CPPCC-Mitglied Lian Yuming reichte in Bezug auf Gesetzgebung zur Datensicherheit den „Antrag auf Gesetzgebung zur Datensicherheit“ (März 2018) und den „Vorschlag zur Beschleunigung des Gesetzgebungsprozesses zum Datensicherheitsgesetz (März 2019) ein. Er forderte die zuständigen nationalen Behörden auf, die theoretische Forschung über Datenrecht, Datenrechtssystem und Datenrechtsgesetz zu intensivieren, Konsultationen zur Ausarbeitung des Datensicherheitsgesetzes aktiv

durchzuführen, die Ausarbeitung des Datensicherheitsgesetzes (Entwurf) schneller zu organisieren, die Zuständigkeit für grenzüberschreitenden Datentransfer zu stärken, das Recht, Datensicherheitsbestimmungen zu erlassen, fest im Griff zu haben und unsere Stimme in der internationalen Gemeinschaft hören zu lassen, Chinas Weisheit und Vorschlag für Förderung der Rechtsstaatlichkeit in der globalen Cyberspace-Verwaltung zu liefern. In den Anträgen von Lian werden auch die Hauptelemente beschrieben, die von der Gesetzgebung zur Datensicherheit abgedeckt werden sollen: „Erstens soll der Zweck der Gesetzgebung die Wahrung der staatlichen Sicherheit, der sozialen und öffentlichen Interessen, den Schutz der legitimen Rechte und Interessen von Bürgern, juristischen Personen und anderen Körperschaften sowie Förderung der Offenheit der und Teilhabe an Daten und Entwicklung und Anwendung von Daten umfassen. Zweitens sollen wir Wert auf Sicherheit und Entwicklung gleichermaßen legen und die Grundsätze der Regierungsleitung, der umsichtigen Überwachung, des Schutzes der Innovation, der Einheit von Befugnissen und Verantwortlichkeiten und der Kontrollierbarkeit der Risiken befolgen. Drittens sollen wir den Umfang, den Schwerpunkt und die Aufsichtsbehörden anpassen. Der anzupassende Umfang soll die Sicherheitsgarantie bei der Datenerhebung, -speicherung, -zirkulation und -anwendung abdecken, wobei Daten und Informationen in Bezug auf nationale Interessen, öffentliche Sicherheit, Geschäftsgeheimnisse, Privatsphäre sowie militärische Forschung und Produktion Vorrang haben. Anders als bei der Ausarbeitung des Cybersicherheitsgesetzes ist der Mangel an Regulierungssubjekt die größte Schwierigkeit für die Gesetzgebung zur Datensicherheit. Der vierte Punkt ist das Standardsystem, für das relevante Interessenträger mobilisiert werden sollen, um zunächst vier realisierbare Standards für Datensicherheit zu probieren und festzulegen, nämlich Basisstandards, technische Normen, Managementstandards und Anwendungsstandards für die Datensicherheit. Der fünfte Punkt ist der klassifizierte Schutz, bei dem es sich um ein klassifiziertes Sicherheitssystem handelt und dabei vertrauliche und sensible Daten ein höheres Schutzniveau erhalten und die Klassifizierung der Schlüsselinformationsinfrastruktur der Klassifizierung des Schutzniveaus der Datensicherheit entspricht. Der sechste Punkt ist die Risikobewertung. Es soll ein obligatorisches

Bewertungssystem für Datensicherheitsrisiken eingerichtet und eine Datensicherheitszertifizierung sowie institutionalisierte Datensicherheitstests eingeführt werden. Der siebte Punkt betrifft Einschränkungsbedingungen. Es soll untersucht werden, einschränkende Bestimmungen für vier Datenkategorien festzulegen. Die erste Kategorie sind Daten, die auf Servern in Übersee gespeichert werden können; die zweite Kategorie sind Daten, die auf steuerbaren autonomen Servern innerhalb des Landes gespeichert werden müssen; die dritte Kategorie sind Daten, die als Sicherung gespeichert werden müssen und die vierte Kategorie umfasst Daten, deren Ausfuhr eingeschränkt wird und das Land nicht verlassen dürfen“ (Zhong Guangping 2018).

Außerdem haben Qi Aimin und Pan Jia eine Reihe von gesetzlichen Garantiemechanismen für die Big-Data-Sicherheit vorgeschlagen, nämlich die Grundprinzipien und spezifische Struktur der gesetzlichen Garantiemechanismen für Big-Data-Sicherheit (einschl. allgemeiner Bestimmungen, privatrechtlicher Mechanismen, strafrechtlicher Mechanismen, verwaltungsrechtlicher Mechanismen und völkerrechtlicher Mechanismen). Sie behaupteten, dass es bei der Gewährleistung der Datensicherheit „nicht nur um einen vollständigen und wirksamen Schutz der Daten geht, sondern auch um die Förderung der Entwicklung, Zirkulation und Nutzung von Datenressourcen und um Realisierung eines angemessenen Gleichgewichts zwischen beiden“ (Qi Aimin & Pan Jia 2015). Eine Literaturrecherche ergab, dass Forscher und Gelehrte die Datensicherheitsgesetzgebung hauptsächlich aus drei Richtungen betrachten: Erstens untersuchen sie Grundbegriffe und Grundrechte wie Informationen, Privatsphäre, Daten, Datenrechte und Datenbankrechte; zweitens werden die Hauptprobleme und Herausforderungen sowie deren Vermeidung und Bewältigung in Bezug auf Datensicherheit untersucht. Drittens werden die Notwendigkeit, Durchführbarkeit, der Zeitpunkt, die Bedingungen und mögliche Hindernisse der Datenschutzgesetzgebung erforscht. Diese Forschungsanstrengungen haben das theoretische Ökosystem der Datenschutzgesetzgebung in Bezug auf Vernünftigkeit, Wissenschaftlichkeit, Jurisprudenz und Rechtskunde aufgebaut und die theoretische und rechtliche Grundlage für die Datensicherheitsgesetzgebung auf lokaler und nationaler Ebene gelegt.

Tabelle 5-8 Lokale Gesetzgebung zu Datenrechten in China

Bezeichnung des Gesetzes	Erlassen von	Erlassungszeitpunkt	Zeitpunkt der Umsetzung
Örtliche Vorschriften			
Vorschriften zur Förderung der Entwicklung und Anwendung von Big Data in der Provinz Guizhou	Volkskongress der Provinz Guizhou (einschließlich des Ständigen Ausschusses)	15. 01. 2016	01. 03. 2016
Bestimmungen der Stadt Guiyang über offene und gemeinsame Regierungsdaten	Volkskongress der Stadt Guiyang (einschließlich des Ständigen Ausschusses)	11. 04. 2017	01. 05. 2017
Vorschriften zum Big Data Security Management der Stadt Guiyang	Volkskongress der Stadt Guiyang (einschließlich des Ständigen Ausschusses)	02. 08. 2018	01. 10. 2018
Vorschriften zur Anwendung und Entwicklung von Big Data im Gesundheitswesen Stadt Guiyang	Volkskongress der Stadt Guiyang (einschließlich des Ständigen Ausschusses)	09. 10. 2018	09. 01. 2019
Vorschriften zur Förderung der Entwicklung und Anwendung von Big Data Tianjin	Volkskongress der Stadt Tianjin (einschließlich des Ständigen Ausschusses)	14. 12. 2018	09. 01. 2019
Bestimmungen zur Kontrolle der Big-Data-Sicherheit Provinz Guizhou	Volkskongress der Stadt Guiyang (einschließlich des Ständigen Ausschusses)	01. 08. 2019	01. 10. 2019
Bestimmungen über Öffnung und Teilhabe der Regierungsdaten Provinz Guizhou (Entwurf)	Volkskongress der Stadt Guiyang (einschließlich des Ständigen Ausschusses)	—	—

Tabelle 5-8 Fortsetzung

Bezeichnung des Gesetzes	Erlassen von	Erlassungszeitpunkt	Zeitpunkt der Umsetzung
Vorschriften und Regeln der regionalen Regierungen			
Maßnahmen zur Verwaltung des Austauschs und der Teilhabe von Geodaten Provinz Zhejiang	Volksregierung der Provinz Zhejiang	04. 05. 2010	01. 07. 2010
Maßnahmen zur Verwaltung des Austauschs und der Weitergabe von Geodaten Provinz Qinghai	Volksregierung der Provinz Qinghai	14. 10. 2015	01. 12. 2015
Maßnahmen zur Verwaltung von Regierungsdaten Provinz Fujian	Volksregierung der Provinz Fujian	15. 10. 2016	15. 10. 2016
Maßnahmen zur Verwaltung von Geodaten Provinz Hunan	Volksregierung der Provinz Hunan	03. 03. 2017	01. 04. 2017
Maßnahmen zur Verwaltung öffentlicher Daten und E-Regierung Provinz Zhejiang	Volksregierung der Provinz Zhejiang	16. 03. 2017	01. 05. 2017
Maßnahmen zur Verwaltung von Regierungsdaten der Stadtregierung Guiyang	Volksregierung der Stadt Guiyang	23. 11. 2017	01. 01. 2018
Maßnahmen zur Verwaltung von Geoinformationsdaten Provinz Jiangxi	Volksregierung der Provinz Jiangxi	26. 12. 2017	01. 03. 2018
Maßnahmen zur Teilhabe und Öffnung von Regierungsdaten der Stadtregierung Guiyang	Volksregierung der Stadt Guiyang	12. 01. 2018	01. 03. 2018

(Fortsetzung)

Tabelle 5-8 Fortsetzung

Bezeichnung des Gesetzes	Erlassen von	Erlassungszeitpunkt	Zeitpunkt der Umsetzung
Maßnahmen zur Verwaltung und Anwendung von öffentlichen Daten der Stadt Chengdu	Volksregierung Chengdu	06. 06. 2018	01. 07. 2018
Vorläufige Maßnahmen zur Prüfung der Teilhabe und Öffnung von Daten der Stadtregierung Guiyang	Volksregierung der Stadt Guiyang	27. 06. 2018	01. 09. 2018
Maßnahmen zur Verwaltung und Teilhabe von Regierungsdaten-ressourcen des autonomen Gebiets der Hui-Nationalität Ningxia	Volksregierung des autonomen Gebiets der Hui-Nationalität Ningxia	04. 09. 2018	01. 11. 2018
Maßnahmen zur Verwaltung von öffentlichen Daten und Internetbüro der Stadt Shanghai	Volksregierung Shanghai	30. 09. 2018	01. 11. 2018
Vorläufige Maßnahmen zur Verwaltung von Big Data der Provinz Hainan	Volksregierung der Provinz Hainan	21. 05. 2019	21. 05. 2019
Maßnahmen zur Verwaltung der Datensicherheit Tianjin(vorläufig)	Büro für Internet und InformationTianjin	26. 06. 2019	01. 08. 2019
Vorläufige Maßnahmen zur Verwaltung von Regierungsdatenressourcen der Stadt Chongqing	Volksregierung der Stadt Chongqing	31. 07. 2019	31. 07. 2019
Vorläufige Maßnahmen zur Öffnung öffentlicher Daten der Stadt Shanghai	Volksregierung Shanghai	29. 08. 2019	01. 10. 2019

(III) System der digitalen Regierungsverwaltung

Die chinesische Regierung misst der Cybersicherheit und Informatisierungsarbeit große Bedeutung bei und hat eine Reihe wichtiger Vorkehrungen getroffen, um den Aufbau eines digitalen China zu beschleunigen. Der 13. Fünfjahresplan schlug die Strategie vor, Chinas Stärke durch netzwerkbasierter Entwicklung auszubauen und die Entwicklung eines digitalen China zu beschleunigen. Im „Programm der nationalen Strategie zur Informatisierungsentwicklung“ werden der Aufbau des digitalen China und die Entwicklung der Informationswirtschaft als oberste Priorität der Informatisierungsarbeit angesehen. Die „nationale Informatisierung im 13. Fünfjahresplan“ hat die Ziele der Entwicklung des digitalen China verfeinert. Im Bericht des 19. Nationalen Kongresses der KP Chinas wurden Anforderungen an den Aufbau des digitalen China weiterhin gestellt (E-Regierung-Forschungszentrum der Parteischule des Zentralkomitees der KP Chinas 2019). Auf der gerade abgeschlossenen vierten Plenarsitzung des 19. Zentralkomitees der KP Chinas wurde dann ein klarer Vorschlag zur Förderung des Aufbaus einer digitalen Regierung gemacht. Als integraler Bestandteil der digitalen China-Kampagne bietet die digitale Regierung strategische Unterstützung für die Modernisierung des staatlichen Verwaltungssystems und der Verwaltungskapazität. Die digitale Regierungsführung ist ein wichtiger Bestandteil der „Regierungsverwaltung in China“. Die digitale Regierungsverwaltung ist ein neues Modell der öffentlichen Verwaltung, das das Verwaltungsniveau mit der modernen Wissenschaft und Technologie in Einklang bringt und auch eine Form der öffentlichen Verwaltung im Einklang mit den Grundbedürfnissen der Öffentlichkeit an Dienstleistung und Rechtsansprüchen im Zeitalter der digitalen Zivilisation. Im Vergleich zum traditionellen Verwaltungsmodell stellt die digitale Regierungsverwaltung eine Reihe von neuen Änderungen und Merkmalen dar: Die Verwaltung wandelt vom geschlossenen zu offenem Modell, von einseitigem zu synergetischem Betrieb und von machtbasierter zu datenbasierter Verwaltung.

Mit dem weiteren Fortschritt der Strategie für „digitales China“ haben Provinzen wie Guangxi, Guangdong, Zhejiang, Hubei und Fujian nacheinander Entwicklungspläne für digitale Regierung oder relevante Richtlinien und Vorschriften bekannt gegeben (siehe Tabelle 5-9). Die Volksregierung der autonomen Region der Zhuang-Nationalität Guangxi hat am 29. August 2018 den „Dreijahresaktionsplan von Guangxi zur Förderung der Entwicklung digitaler Regierung“ (2018–2020) herausgegeben, in dem das Arbeitsziel vorgeschlagen wird, „zunächst eine digitale Regierung mit wissenschaftlich fundierten Entscheidung und Analyse, verfeinertes internes Management und hocheffiziente Bereitstellung öffentlicher Dienste bis 2020 zu errichten“ und spezifische Vorkehrungen für sieben Hauptaufgaben, nämlich Förderung des Aufbaus eines integrierten Basisunterstützungssystems, Förderung des offenen Zugangs zu und Teilhabe an Datenressourcen, Förderung der „Internet-Plus-Regierungsdienstleistung“, Förderung der Big-Data-Anwendung für Makroentscheidung, Förderung der digitalisierten Marktaufsicht, Förderung der digitalisierten Aufsicht über natürliche Ressourcen und Förderung der digitalisierten Regulierung der ökologischen Umwelt.

Die Volksregierung der Provinz Guangdong veröffentlichte am 26. Oktober 2018 den „Gesamtplan der Provinz Guangdong für den Aufbau ‚digitaler Regierung‘“ (2018–2020) und schlug vor, dass Guangdong bis Ende 2020 ein Verwaltungssystem der „digitalen Regierung“ mit einem ganzheitlichen Vorantrieb, der Regierung-Unternehmenskooperation und Trennung von Management und Betrieb und ein digitales Regierungsgeschäftssystem, das Gesamtbetrieb, Teilhabe und Synergie sowie Service-Integration umfasst, aufbaut, ein einheitliches und sicheres Regierungs-Cloud und Regierungsnetzwerk erstellt, ein offenes und integriertes Big-Data-Zentrum und eine integrierte Online-Regierung auf Service-Plattform errichtet und eine „digitale Regierung“ bildet, die oben mit allen staatlichen Organen und unten mit Stadt- und Kreisstellen des Regierungssystems verbunden ist und alle horizontalen Bereiche und vertikalen Aspekte abdeckt. Am 28. Dezember 2018 veröffentlichte die Volksregierung der Provinz Zhejiang die „Reform der Provinz Zhejiang für Regierungsdienste all aus einer Hand und einen

Gesamtplan für die digitalisierte Transformation der Regierung“. Das vorgeschlagene Gesamtziel besteht darin, zunächst ein digitales Regierungssystem bis Ende 2020 zu bilden, das vertikal gut durchgängig und horizontal synergetisch ist und eine Verbindung oben zu allen staatlichen Organen und unten mit einer Abdeckung aller Aspekte und Bereiche der ganzen Provinz bietet. Der Gesamtrahmen der digitalen Regierung ist eine Datenplattform mit „vier horizontalen und drei vertikalen Linien“, und die hierarchische Struktur wird mit einem Gleichgewicht zwischen Integration und Arbeitsteilung gebaut. Im Januar 2019 gab die Volksregierung der Provinz Hubei die „Leitmeinungen der Volksregierung der Provinz Hubei zur Förderung der Entwicklung digitaler Regierung“ und den „Umsetzungsplan der Provinz Hubei zur Förderung der Entwicklung digitaler Regierung“ heraus, in dem spezifische Vorkehrungen in fünf Aspekten getroffen wurden: intensive Unterstützung der Infrastruktur, Integration von Regierungsdiensten, intelligente Integration der kooperativen Büroarbeit, wissenschaftlich fundierte Regierungsentscheidung für Regierungsführung und systematische Unterstützung mit soliden Arbeitsmechanismen. Am 20. März 2019 führte die Volksregierung der Provinz Fujian „wichtige Arbeitspunkte von Digital Fujian 2019“ ein, in denen spezifische Anforderungen in fünf Aspekten gestellt wurden: alle Anstrengungen zu unternehmen, um den Erfolg des zweiten Digital China-Gipfels sicherzustellen, die Informationsinfrastruktur zu optimieren und aktualisieren, umfassende Verbesserung der E-Regierungsdienste, Umsetzung des Aktionsplans für Führung in der digitalen Wirtschaft und Stärkung der Unterstützung für eine wirksame Umsetzung (E-Regierung-Forschungszentrum der Parteischule des Zentralkomitees der KP Chinas 2019).

Tabelle 5-9 Pläne der lokalen digitalen Regierung in China

Bezeichnung	Herausgegeben	Zeitpunkt der Veröffentlichung
Dreijähriger Aktionsplan von Guangxi zur Förderung der Entwicklung der digitalen Regierung (2018–2020)	Volksregierung der autonomen Region der Zhuang-Nationalität Guangxi	29. 08. 2018
Masterplan der Provinz Guangdong für den Aufbau einer digitalen Regierung (2018–2020)	Volksregierung der Provinz Guangdong	26. 10. 2018
Reform der Provinz Zhejiang für Regierungsdienste aus einer Hand und Gesamtplan für die digitale Transformation der Regierung	Volksregierung der Provinz Zhejiang	28. 12. 2018
Leitmeinungen der Volksregierung der Provinz Hubei zur Förderung der Entwicklung digitaler Regierungen	Volksregierung der Provinz Hubei	15. 01. 2019
Umsetzungsplan der Provinz Hubei zur Förderung der Entwicklung der digitalen Regierung	Volksregierung der Provinz Hubei	15. 01. 2019
Umsetzungsplan für die Entwicklung der digitalen Regierung in der Provinz Shandong (2019–2022)	Volksregierung der Provinz Shandong	13. 03. 2019
Wichtige Arbeitspunkte von Digital Fujian im Jahr 2019	Volksregierung der Provinz Fujian	20. 03. 2019
Arbeitsplan zur Beschleunigung der Entwicklung der digitalen Regierung in der autonomen Region Ningxia Hui	Volksregierung der autonomen Region Ningxia Hui	24. 06. 2019

Die Öffnung von und Teilhabe an Regierungsdaten ist eine der dringenden Aufgaben einer digitalen Regierungsverwaltung. Auf nationaler Ebene hat China am 5. April 2007 die „Verordnung über Öffnung der Regierungsinformationen“ offiziell erlassen, in der alle Verwaltungsbehörden aufgefordert sind, Regierungsinformationen gemäß den gesetzlichen

Verfahren der Öffentlichkeit zugänglich zu machen. Am 31. August 2015 veröffentlichte der Staatsrat den „Aktionsplan zur Förderung der Big-Data-Entwicklung“ mit dem Vorschlag, „den Aufbau einer einheitlichen nationalen offenen Regierungsdatenplattform zu beschleunigen und Pläne für öffentliche Institutionen zur Veröffentlichung ihrer Daten zu erstellen“. Am 5. September 2016 erließ der Staatsrat die „vorläufigen Maßnahmen für Verwaltung der Teilhabe an Regierungsinformationsressourcen“, in denen einheitliche Bestimmungen für Teilhabe an Regierungsinformationen auf nationaler Ebene festgelegt wurden, um die stückweise Trennung zwischen verschiedenen Verwaltungsorganen, die isoliert handeln, aufzuheben. Es ist zwingend festgelegt, wenn Ressourcen nicht teilhabbar sind, muss es triftigen Grund geben, damit kann vermieden werden, dass Verwaltungsbehörden die Teilhabe an Ressourcen ohne Grund verweigern. Im Oktober 2019 wurde auf der vierten Plenarsitzung des 19. Zentralkomitees der KP Chinas vorgeschlagen, „den Aufbau einer landesweit integrierten Plattform für Regierungsdienste zu beschleunigen“, damit Regierungsstellen den Unternehmen und der Öffentlichkeit öffentliche Dienstleistungen anbieten können, die das gesamte Gebiet abdecken und den ganzen Prozess besser integrieren, was zur Modernisierung der Regierungsverwaltung beiträgt. Mit der Verbesserung der nationalen Regierungskapazitäten und der raschen Entwicklung der sozialen Informatisierung stießen die „Verordnungen über offene Regierungsinformation“ (2008) auf Probleme in der neuen Situation im Umsetzungsprozess. Daher hat der Staat im Jahr 2019 die „Verordnungen über offene Regierungsinformation“ überarbeitet und vervollständigt. Die überarbeitete Ausgabe trat am 15. Mai 2019 in Kraft. Diese Änderungen betreffen hauptsächlich drei Aspekte: Erstens werden wir uns an den Grundsatz halten, dass alle Regierungsinformationen normalerweise offen sind, es sei denn, wenn einige als Ausnahme nötigerweise vertraulich zu behandeln sind. Der Umfang offener Regierungsinformationen muss klar definiert und die aktive Öffnung ständig erweitert werden. Zweitens werden wir das Verfahren zur Offenlegung auf gesetzmäßiger Anfrage verbessern, um die legitimen Rechte und Interessen von Antragstellern und anderen Interessengruppen wirksam zu schützen, während notwendige Maßnahmen auch gleichzeitig ergriffen werden, um zu verhindern, dass

einige Antragsteller ihr Recht auf Informationsantrag nicht ordnungsgemäß ausübt und der normale Betrieb offener Regierungsinformationen dadurch behindert würde. Drittens sollen strengere Anforderungen an bürgerbequeme Dienstleistung gestellt werden, um die Wirksamkeit der Offenlegung von Regierungsinformationen durch den Einsatz von Informationstechnologie zu steigern, und die Rolle der Regierungsinformationen als Dienstleister für die Produktion, das tägliche Leben, die wirtschaftlichen und sozialen Aktivitäten der Volksmassen voll auszuspielen (Wu Shan 2019).

Auf lokaler Ebene gaben Beijing, Wuhan und Shanghai 2008, 2015 und 2016 ihre Verwaltungsmaßnahmen zur Teilhabe an Regierungsdatenressourcen einander folgend heraus (siehe Tabelle 5-10). 2017 führte Guiyang die „Bestimmungen über Teilhabe an offenen Regierungsdaten“ ein, die als Erste ihrer Art auf lokaler Ebene in China erfordert, die Regierungsdaten der Öffentlichkeit offenzulegen und die Arbeit, Finanzmittel und zielgerichtete Leistungsbewertung in Bezug auf Öffnung von und Teilhabe an Regierungsdaten auf gesetzlicher Weise zu verwalten, um nachhaltige Entwicklung der Öffnung von und Teilhabe an Regierungsdaten sicherzustellen. Die Umsetzung dieser Verordnungen bedeutet, dass die Öffnung von und Teilhabe an Regierungsdaten nicht länger eine Frage des Wunsches oder des Willens ist, sondern ist es ein Muss nach dem Gesetz, die Öffnung von und Teilhabe an Regierungsdaten gesetzmäßig und ordnungsgemäß durchzuführen. Ermutigt durch diese Verordnungen hat die „offene Regierungsdatenplattform Guiyang“ als erste integrierte offene Regierungsdatenplattform auf Stadtebene in China zum 13. November 2019 insgesamt 11.729.739 Dateneinträge, 3.078 Datensätze und 480 Schnittstellen zur Programmierung von Anwendungen (APIs) von 51 Kommunalbehörden und 13 Distrikten und Landkreisen offengelegt.¹⁵ Jeder kann Regierungsdaten von der Plattform auf Weise nach Thema, Branche, Gebiet, Abteilung oder Bezirk / Landkreis suchen und abrufen. Im Mai 2019 veröffentlichte Provinz Guizhou den „Entwurf für Kommentar zu den Bestimmungen der Provinz Guizhou über Teilhabe an offenen

15 Daten sind auf der Guiyang Open Regierung Data Platform unter <<http://www.gyopendata.gov.cn/city/index.htm>> verfügbar.

Regierungsdaten“ (im Folgenden kurz als „Verordnungsentwurf“ genannt), der 44 Artikel in acht Kapiteln enthält und hat klare Bestimmungen in Bezug auf Verwaltung, Teilhabe, Offenheit, Anwendung, Aufsicht und gesetzliche Verbindlichkeiten der Regierungsdatenressourcen festgelegt. In Bezug auf Datenteilhabe ist im „Verordnungsentwurf“ eindeutig festgelegt, dass die Datenteilhabe dem Grundsatz „Teilhabe als Prinzip und Nicht-Teilhabe als Ausnahme“ folgt. Die Datenteilhabe ist in drei Kategorien unterteilt: die bedingungslose Teilhabe, bedingte Teilhabe und Nicht-Teilhabe. In ähnlicher Weise wird auch die Offenlegung der Regierungsdaten basierend auf den drei Kategorien angeboten: bedingungslose und bedingte Offenlegung und Nicht-Offenbarung. Auf diese Weise hat Guizhou den „Schlüssel“ zur Big-Data-Gesetzgebung für Offenlegung der Regierungsdaten erfasst. Der offene Zugang zu und die Teilhabe an Regierungsdaten sind wegweisend für den gesellschaftsweiten offenen Zugang und Teilhabe und bieten die „Erfahrungen von Guizhou“, die in ganz China kopierbar und verbreitbar sind.

Außerdem führt man die Teilhabe an Regierungsdaten zwischen verschiedenen Verwaltungsstellen im Gebiet Taiwan China bereits seit mehreren Jahren durch. Seit 2013 werden die Richtlinien für Offenheit der Regierungsdaten aktiv umgesetzt und eine Reihe von „Durchführungsbestimmungen für Offenheit der Regierungsdaten“ erlassen wie die „Grundsätze für Operation der Öffnung der Regierungsunterlagen“, „Wichtige Punkte der Verwaltung der Öffnung von Regierungsunterlagen“, „Vorschriften für Verwendung der Unterlagen auf der Öffnungsplattform der Regierungsunterlagen“ und „Bestimmungen für Autorisierung der Öffnung der Regierungsunterlagen – erste Version“. Am 09.12.2015 wurde das Ergebnis der internationalen Beurteilung von Offenheit der Regierungsdaten durch die „Stiftung der offenen Kenntnisse“ bekannt gegeben: das Gebiet Taiwan hat den ersten Platz genommen (Lian Yuming 2017, S. 88).

Tabelle 5-10 System für Teilhabe und Öffnung der Daten der regionalen Regierungen in China

Ort	Dokumentsbezeichnung	Wichtige Punkte	Jahr
Beijing	Einige Stellungnahmen zur Stärkung der Teilhabe an Regierungs- informationsressourcen	Allgemeiner Plan für Aufbau und Pflege der Informationsressourcendatenbank. Es vermeidet wiederholte Arbeiten durch Teilhabe und Suchweise und legt klare Regeln für die Verantwortlichkeit der Datenerfassung fest. Auf der Grundlage von Vertraulichkeitsvereinbarung, die zwischen dem Anbieter und dem Benutzer unterzeichnet wurden, müssen alle Informationsressourcen rechtzeitig und kostenlos weitergegeben werden.	2005
	Vorschriften zur Förderung der Informatisierung der Stadt Peking	Es legt Regeln für Verwaltung von Regierungsinformationen, die Integration bestehender Informatisierungsprojekte, den Aufbau einer einheitlichen Plattform für den Austausch von Regierungsinformationen, Leitlinien und die Standardisierung der Nutzung von Informationsressourcen zur Wertschöpfung und eine verbreitete Anwendung von Informationstechnologie und die effektive Implementierung des klassifizierten Sicherheitsschutzes fest.	2007
	Maßnahmen zur Verwaltung der Plattform für den Austausch und Teilhabe von Informationsressourcen der Stadt Peking	Alle kommunalen Behörden müssen Ressourcen über die kommunale Teilhabe- und Austauschplattform gemeinsam nutzen, und verschiedene Plattformen für die gemeinsame Nutzung von Distrikten und Landkreisen sind mit der kommunalen Plattform verbunden. Es legt fest, dass diejenigen, die Daten anfordern, die teilhabbaren Daten ohne Erlaubnis nicht an Dritte weitergeben dürfen, und betont die Anforderungen auf den sicheren Betrieb und die Wartung der Teilhabepattform.	2008

	Meinung zur Durchführung der Förderung des Informationsverbrauchs und Vergrößerung der inneren Nachfrage	Steigerung der Fähigkeit für Informationsverbrauch und -angebot, Vorantrieb der Branchenaufwertung, Vervollständigung der Info-Infrastruktur der neuen Generation, Förderung der Teilhabe an öffentlichen Informationsressourcen und Ermutigung der gesellschaftlichen Mehrwert-Entwicklung.	2014
	Aktionsplan für Big Data und Cloud-Computing Beijing	Vorschlag für Zielsetzung zu Datenoffenheit, bis 2020 sollen Öffnungseinheiten 90% und Datenöffnungsrate 60% jeweils erreichen, zugleich soll die Qualität der Datenöffnung und Nutzungseffizienz erhöht werden.	2016
	Plan für Entwicklung der Informatisierung im Zeitraum des 13. Fünfjahresplans Beijing	Erstellung von Plan und Liste für Teilhabe an öffentlichen Daten; Anleitung der Öffnung und Integration der Sozialdaten durch Öffnung öffentlicher Daten	2016
Shanghai	Dreijahresaktionsplan für Förderung der Forschung und Entwicklung von Big Data (2013–2015)	Analyse der Vorteile und Unzulänglichkeit von Shanghai, Vorteile sind reichliche Datenressourcen, starke Forschungskapazität und erste Kontur der Datenbranche; Schwachstellen sind unzureichende Datenindustrie, nicht ausreichende Reserve der Schlüsseltechnologien, ohne vollständige Branchenkette; Vorschlag für Förderungsmechanismus zur Spezifizierung der Datenteilhabe durch Vertragsabschluss	2013
	Umsetzungsgutachten zur Förderung des offenen Zugangs zu und der Nutzung von Informationsressourcen der Regierung der Stadt Shanghai	Es sind anwendungsorientierte, aktive, umsichtige und schrittweise Maßnahmen zu treffen, um den offenen Zugang zu Daten zu fördern, die mit Steuermitteln erstellt und gesammelt werden. Für Daten, die veröffentlicht werden sollen, aber aufgrund unreifer Bedingungen nicht veröffentlicht werden können, sollen erforderliche Bedingungen für Offenlegung solcher Daten geschaffen werden und soziale Kräfte sollen ermutigt werden, Entwicklungsaktivitäten zur Wertschöpfung durchzuführen.	2014

(Fortsetzung)

Tabelle 5-10 Fortsetzung

Ort	Dokumentsbezeichnung	Wichtige Punkte	Jahr
	Arbeitsplan für Teilhabe und Öffnung von Datenressourcen im Zusammenhang mit Regierungsangelegenheiten für das Jahr 2015 der Stadt Shanghai	Es erfordert Anstrengungen zur Verbesserung der drei Basisdatenbanken; alle Stadtbehörden werden aufgefordert, ihre Datenressourcen zu sortieren und Liste für Datenoffenheit gemäß den für 2015 festgelegten Schlüsselbereichen zu erstellen; erfordert Anstrengungen, um soziale Bedürfnisse zu ermitteln und zu analysieren und die Qualität von Datendiensten zu verbessern und andere Kanäle für den Zugriff auf öffentliche Daten als das Datendienstnetz zu erweitern.	2015
	Arbeitsplan für Eröffnung und Teilhabe von Datenressourcen im Zusammenhang mit Regierungsangelegenheiten für das Jahr 2016 der Stadt Shanghai	Neue Informatisierungsprojekte, die Daten Teilhabe nicht unterstützen, werden nicht genehmigt. Auf dynamische Echtzeitdaten wird hauptsächlich über Schnittstellen zugegriffen; sensible Daten werden nach der Desensibilisierung veröffentlicht. Daten mit höheren Sicherheitsstufen, wie z.B. sicherheitsrelevante Daten, werden auf Anfrage gesetzlich zur Verfügung gestellt; Arbeit für Teilhabe und Öffnung wird in die Leistungsbewertung einbezogen. Die „Stadt-sicherheit“ ist der Schlüsselbereich der Datenöffnung des Jahres 2016.	2016
	Implementierungsmeinungen zur Big-Data-Entwicklung in Shanghai	Setzt Standards für offene Datensysteme, stärkt das Qualitätsmanagement und die Gegenprüfung, nimmt Offenheit und Teilhabe in Leistungsbewertung auf, fördert den offenen Zugang zu und Teilhabe an Sozialdaten und leitet kommerziellen Datenverkehr.	2016
	Verwaltungsmaßnahmen für Teilhabe an Regierungsdatenressourcen der Stadt Shanghai	Definiert Verantwortlichkeit und Arbeitsteilung für Datenteilhabe, verlangt von Verwaltungsinstitutionen, Daten nicht wiederholt zu erfassen, legt Regeln für die klassifizierte Teilhabe fest, die in drei Kategorien geteilt ist: freie Teilhabe, Teilhabe auf Anfrage und nicht teilhabbar.	2016

Guiyang	Einige Stellungnahmen zur Beschleunigung der Entwicklung der Big-Data-Branche	Vorgeschlagen, bis 2017 die weltweit erste öffentliche Plattform für Blockdaten aufzubauen.	2015
	Bestimmungen zur Offenlegung von Regierungsinformationen Guiyang (überarbeitet)	Neue Anforderungen an Regierungsbehörden auf verschiedenen Ebenen, um die Informationsteilnahme zu fördern	2015
	Zehn Maßnahmen zur Förderung von Innovationen der Big-Data-Technologie in der nationalen High-Tech-Entwicklungszone in Guiyang	Ermutigt und belohnt Unternehmen, offene Daten zu entwickeln und zu nutzen, und lädt Benutzer dazu ein, ihre „unangenehmen Erfahrungen“ zu teilen, um „Schmerzpunkte“ zufriedenstellende zu beseitigen	2016
	Arbeitsplan zur Kopie experimenteller Praktiken der Pilot-Freihandelszone Chinas (Shanghai) der Stadtregierung Guiyang	Erfordert Sammlung, Kommunikation und Benutzung von Regierungsdaten; Einrichtung eines gemeinsamen Versammlungssystems für Arbeit der Datenteilnahme	2016
	Bestimmungen über Öffnung und Teilnahme der Regierungsdaten der Stadt Guiyang	Teilhabbare Daten von Lizenzen und Bescheinigungen können als Verwaltungsbelege gelten, Listen für Teilnahme und Offenheit der Daten werden sozial bekannt gegeben, offene Daten werden auf einer offenen Datenplattform auf maschinenlesbare und reproduzierbare Weise bereitgestellt und Daten, die geöffnet werden sollen, aber noch nicht geöffnet worden sind, ob die innerhalb oder außerhalb der Listen sind, können auf Anfrage geöffnet werden.	2017

(Fortsetzung)

Tabelle 5-10 Fortsetzung

Ort	Dokumentsbezeichnung	Wichtige Punkte	Jahr
Wuhan	Meinungen zur Förderung der Big-Data-Anwendung und zur Entwicklung der Big-Data-Branche	Vorschlägen, die Datenbestände der Stadtregierung aufzuzeichnen, Datenaustauschplattformen und Handelsmärkte aufzubauen, Demonstrationsprojekte für Anwendungen durchzuführen, die Gesellschaft bei der Erfassung offener Daten zu unterstützen, die Regierungsvorschriften und das Sicherheitssystem zu verbessern.	2014
	Aktionsplan zur Entwicklung der Big-Data-Industrie (2014–2018) von Wuhan	Die Regierungsdaten sollen zuerst geöffnet werden, Regierungsdatenbestände zentral zu verwalten, Regeln für Datentransaktionen festzulegen und auf der Grundlage von Handelsplattformen eine Big-Data-Industriekette zu bilden.	2014
	Vorläufige Maßnahmen zur Verwaltung der Teilhabe von Regierungsdatenressourcen der Stadt Wuhan	Verwaltungsinstitutionen sollen die digitale Transformation und strukturierte Datenverarbeitung durchführen. Daten von Lizenzen und Bescheinigungen sollen mit elektronischen Siegeln versehen und in Echtzeit aktualisiert werden. Die Daten sind in drei Kategorien unterteilt: uneingeschränkt Teilhabe, eingeschränkte Teilhabe und nicht-teilhabebar.	2015
Taiwan, China	Gesetz über Offenlegung der Regierungsdaten	Regierungsinformationen sollen aktiv offengelegt oder auf Anfrage zur Verfügung gestellt werden. Regierungsbehörden können Gebühren entsprechend dem Zweck der Beantragung auf Regierungsdaten erheben. Der Gebührenstandard wird von jeder Agentur festgesetzt. Diejenigen, die Regierungsdaten für Zwecke akademischer Forschung oder Zwecke des Gemeinwohls beantragen, können eine Zinssenkung oder Befreiung beantragen.	2005

	<p>Grundsätze für Öffnungsarbeit der Regierungsdaten</p>	<p>Nach dem Grundsatz der Offenheit können sensible Informationen und andere besondere Umstände Ausnahmen sein, wenn die Gründe formell und mit Zustimmung der zuständigen Verantwortlichen angegeben werden. Die „zentralen Behörden der zweiten Ebene“ sollen als Zentren für die Gesamtplanung dienen und die Daten auf der offenen Datenplattform der Regierung auflisten. Wenn ein Datensatz veröffentlicht wird, darf er nicht willkürlich in Teile unterteilt werden, um seine Integrität, Richtigkeit und Aktualität sicherzustellen. Prinzipiell werden sie kostenlos bereitgestellt und für Personen mit besonderen geschäftlichen Anforderungen, werden die Abrechnungsmethode und der Betrag vereinbart. Alle Agenturen legen auf der Basis des Grundsatzes der Nutzung zur Wertschöpfung Standards und Beschränkungen für Nutzung von Daten fest. Alle Behörden richten eigenen Mechanismus für Leistungsmanagement und Leistungsförderung ein.</p>	<p>2013</p>
	<p>Wichtige Punkte der Verwaltung der Öffnung von Regierungsdaten</p>	<p>Mit Abteilungen als Zentren wird Datensatzverwaltung aller nachgeordneten Stellen koordiniert geplant.</p>	<p>2013</p>
	<p>Bestimmungen für Nutzung der Daten auf offener Plattform der Regierungsinformationen</p>	<p>Die Autorisierung soll kostenfrei und nicht ausschließlich erfolgen und darin keine Marken- und Patentrechte beinhalten und auch keine Einschränkung der Zeit, des Ortes und der Art der Nutzung für den Benutzer darstellen. Wenn Benutzer Fehler und Auslassungen finden, sollen sie kostenlos Informationen bereitstellen, um Regierungsbehörden bei der Korrektur zu unterstützen. Der Benutzer haftet für den Ersatz von Schäden an den Interessen Dritter; Regierungsbehörden übernehmen keine Garantie für die Vollständigkeit und Richtigkeit der Daten.</p>	<p>2013</p>
	<p>Autorisierungsbestimmung für Öffnung der Regierungsdaten Taiwan 1.0</p>	<p>Benutzer dürfen keine Unterautorisierung vornehmen. Die Nutzer sollen die ursprüngliche Datenlieferungsbehörde deutlich angeben.</p>	<p>2015</p>

Abschnitt III Sonderbedeutung des Datenrechtssystems für die globale Internetverwaltung

Das Datenrechtsgesetz ist ein wichtiges Rechtsinstrument für ein Land zur Teilnahme an der globalen Verwaltung und ein „goldener Schlüssel“ für Lösung von Problemen der globalen Cyberspace-Verwaltung. Gegenwärtig ist die Entwicklung des globalen Cyberspace-Verwaltungs-Systems unausgewogen, relevante Regeln sind nicht vollständig, die Cyberspace-Ordnung ist nicht rational, die Struktur ist abnormal, in der Hegemonie herrscht und Rechtsstaatlichkeit unterentwickelt ist (Zhi Zhenfeng 2017). Die technologische Gemeinschaft scheint von sich aus Regeln spontan zu erlassen, wird jedoch von Anfang an von technisch hegemonialen Mächten manipuliert, weshalb ein Machtmonopol unter dem Deckmantel der „Pseudodezentralisierung“ im globalen Internet herrscht. Das Internet ist kein Ort außerhalb des Gesetzes, und die internationale Gemeinschaft benötigt ein faires rechtsstaatliches System im Cyberspace. Auf der Grundlage des theoretischen Rahmens von „Datenrecht-Datenrechtssystem-Datenrechtsgesetz“ werden wir daher hiermit den Aufbau einer Schicksalsgemeinschaft mit gemeinsamer Zukunft im Cyberspace näher erläutern und die besondere Bedeutung des Datenrechtsgesetzes für Förderung der globalen Cyberspace-Verwaltung tiefgehend untersuchen, um einen Weg zur Rechtsstaatlichkeit im Cyberspace mit einem „chinesischen Ansatz“ anzubahnen.

(I) Weltweite Bedeutung des Datenrechtsgesetzes

1. Änderung der Idee: vom Grenzmanagement zur souveränen Verwaltung

Die Souveränität ist das Kernthema der globalen Internetverwaltung. Die Cyber-Souveränität¹⁶ ist ein wichtiger Eckpfeiler der Reform des

16 Die Cyber-Souveränität wurzelt in der modernen Rechtsphilosophie und gilt als natürliche Erweiterung und Repräsentation der nationalen Souveränität im Cyberspace. Sie ist ein wichtiger Bestandteil der nationalen Souveränität.

globalen Internetverwaltungssystem und der Verwirklichung der guten und gesetzmäßigen Verwaltung. Die Achtung der Cyber-Souveränität bedeutet, sich der Cyber-Hegemonie zu widersetzen. In Bezug auf die globale Cyberspace-Verwaltung konzentrieren sich die traditionellen rechtlichen und technologischen Regelungen auf das Grenzmanagement im Internet und die Einrichtung selbstständiger und kontrollierbarer Methoden zur Routenauthentifizierung. Im Zeitalter von Big Data wird der Wettbewerb zwischen verschiedenen Interessengruppen um die Kontrolle über Daten jedoch immer härter. Die traditionellen Grenzen des Cyberspace-Managements zwischen Staaten, Unternehmen und Einzelpersonen werden allmählich durchbrochen. Es ist dringend erforderlich, eine Reihe globaler Gesetze basierend auf souveräner Verwaltung neu zu definieren, die Beziehungen in Bezug auf Dateneigentumsrecht zu versöhnen und zu optimieren. Als zentraler Kernelement und wichtige Konnotation des Datenrechtsgesetzes ist die Cyber-Souveränität eine wichtige Garantie für das globale Cyberspace-Verwaltungssystem, das die Achtung der Souveränität aller relevanten Länder, den gleichberechtigten Dialog und letztendlich die Verwirklichung des gemeinsamen Aufbaus und der gemeinsamen Teilhabe im Cyberspace umfasst. Das Datenrechtsgesetz betont, dass die globale Cyberspace-Verwaltung auf Verwaltung der Souveränität beruhen muss. Unter der Voraussetzung der Einhaltung der einschlägigen Gesetze und Vorschriften genießen souveräne Staaten im Cyberspace das Zuständigkeitsrecht, das Recht auf Unabhängigkeit, das Recht auf Verteidigung, das Recht auf Gleichheit usw. Nur wenn die Cyberspace-Verwaltung auf souveräner Verwaltung basiert, kann diese wirklich gerecht und fair sein.

2. Institutioneller Wandel: Von der hegemonialen Alleinherrschaft zur Konsultation und Demokratie

Der „Unilateralismus“ ist ein Schlüsselproblem in der globalen Cyberspace-Verwaltung. Die entwickelten Länder im Cyberspace nutzen ihre fortschrittlichen Technologien und starkes Rederecht, treten mutwillig auf internationale Gerechtigkeit, befürworten den Cyberliberalismus, setzen die Strategie der Cyberabschreckung um und fördern mittels Internet die ideologische Hegemonie im Cyberspace. China hält

an den Grundsätzen der großen Struktur und des großen Sichtfeldes mit umfassender Konsultation, gemeinsamer Teilhabe und gemeinsamer Verwaltung im Cyberspace fest und befürwortet Multilateralismus und mehrseitige Beteiligung an der globalen Cyberspace-Verwaltung anstelle von Unilateralismus, Hegemonismus und Diktatur. Dies bedeutet, dass die Cyberspace-Verwaltung auf Konsultationen zwischen verschiedenen souveränen Staaten beruhen soll, wobei die Rolle von verschiedenen Subjekten wie Regierungen, internationalen Organisationen, Internetunternehmen, Technologiegruppen, Nichtregierungsorganisationen, Bürgern usw. voll berücksichtigt werden soll. Das Datenrecht ist in der Natur das Teilhaberecht. Das Datenrechtsgesetz ist ein Rechtsinstrument, das auf dem Datenrechtssystem basiert. Es hat in der Natur Kultur der altruistischen Gene und verfügt über die Basis und Eigenschaft der konsultativen Demokratie. Unter Wahrung der Cyber-Souveränität befürwortet das Datenrechtsgesetz den Multilateralismus, die konsultative Demokratie und internationale Zusammenarbeit, unterstützt die Vereinten Nationen bei der Koordinierung der globalen Cyberspace-Verwaltung, spiegelt die Interessen aller Interessengruppen auf der ganzen Welt voll und ganz wider und zielt darauf ab, „den größten gemeinsamen Teiler herauszufinden und den größten konzentrischen Kreis zu ziehen“ und Hand in Hand eine Schicksalsgemeinschaft mit gemeinsamer Zukunft im Cyberspace gemeinsam aufzubauen.

3. Strukturwandel: Von der Dezentralisierung zur Wiederzentralisierung

Das Internet wurde in den Vereinigten Staaten geboren. Es wird angenommen, dass die Internet-Technologien und -Architektur dem Internet den einzigartigen Charakter der „Dezentralisierung“ verleihen. Dem Wesen nach ist dies jedoch ein Missverständnis. Die „Dezentralisierung“ ist hier keine Dezentralisierung im realen und absoluten Sinne. Es handelt sich dabei vielmehr um eine „Dezentralisierung“ innerhalb der US-zentrierten Struktur. Zum Beispiel sind große Internetbetreiber und Verwaltungsinstitutionen auf der ganzen Welt fast alle in den Händen westlicher Länder mit den Vereinigten Staaten an der Spitze. Dies

könnte viele Interessenträger zum Fehlen an Diskussionsrecht bringen: Erstens würden ihre berechtigten Interessen ungeschützt lassen und zweitens würden ihnen die Autonomie bei der Wahl ihres eigenen Internetentwicklungspfads und -modells entzogen. Das Datenrechtsgesetz, das auf den Aufbau einer Schicksalsgemeinschaft im Cyberspace abzielt, bietet eine Lösung für die gesetzbasierte globale Cyberspace-Verwaltung. Das Datenrechtsgesetz betont, dass das Internet eher eine dezentrale und polyzentrische als eine absolut dezentrale Struktur hat und dass alle souveränen Staaten Identitätsauthentifizierung und Kontoverwaltung auf verschiedenen Knoten basierend auf ihrer eigenen Cyberspace-Souveränität realisieren können. In einer solchen dezentralen und polyzentrischen Cyber-Struktur sind alle Zentren gleich und haben die gleiche Gewichtung, in der es keine Hegemonie oder Alleinherrschaft und auch keine absolute Autorität zwischen den Zentren gibt.

4. Modellwechsel: von technologischer Verwaltung zu guter gesetzlicher Verwaltung

Das Internet hat seinen Ursprung in den Vereinigten Staaten, in dem die Mechanismen und Modelle seiner Verwaltung hauptsächlich auf der spontanen Organisation durch technologische Gemeinschaften basieren. Diese technologischen Gemeinschaften bestehen jedoch meistens aus amerikanischen Organisationen und ihre Kernmanager und Wissenschaftler stammen fast alle aus großen Industrieländern in Europa und Amerika. Sie befürworten Freiheit und technologiebasierte Cyberspace-Verwaltung. Technologie kennt keine Landesgrenze, aber Wissenschaftler haben ihre Nationalität. Die Nationalitäten der Wissenschaftler, die die Kerntechnologien kontrollieren und die lauteste Stimme in der globalen Cyberspace-Verwaltung haben, werden sich direkt auf die Zukunft von Wissenschaft und Technologie und die Cybersicherheit des Landes auswirken. Im Gegensatz dazu befürwortet das Datenrechtsgesetz keine Verwaltung, die ausschließlich auf Technologie basiert. Stattdessen wird betont, dass die globale Cyberspace-Verwaltung einen „kombinierten Faustschlag“ aus gesetzlichen und

technischen Regeln erfordert.¹⁷ Das Wesentliche dieses „kombinierten Faustschlags“ ist die „Wiedervermischung“, dessen Ziel darin besteht, eine „technologiebasierte Verwaltung mit gesetzlichen Regelungen“ zu erreichen. Ihre Kernpunkte sind wie folgend: Erstens Anpassung an die Bedürfnisse der Internet-Technologiearchitektur und der Innovation von Geschäftsmodellen; zweitens Ausgewogenheit und Koordination zwischen verschiedenen Interessengruppen und unterschiedlichen Wertkonzepten sowie drittens die Notwendigkeit, die gesunde Entwicklung der Internetbranche anzuleiten und zu fördern sowie Fairness und Gerechtigkeit aufrechtzuerhalten. Auf dieser Grundlage kann das Datenrechtsgesetz als gemeinsamer Verhaltenskodex und Wertorientierung der Internetgesellschaft dienen, zu einer guten und gesetzmäßigen Regulierung beitragen und die Entstehung einer globalen guten Internet-Ordnung beschleunigen.

(II) Das Dilemma der Gesetzherrschaft in der globalen Internetverwaltung

Die Internetverwaltung ist nicht nur ein wichtiger Bestandteil der globalen Verwaltung, sondern auch ein wichtiger Aspekt des Spiels zwischen Großmächten. Gegenwärtig ist die globale Cyberspace-Verwaltung mit einer unzureichenden Versorgung mit Systemen und einer Rechtsstaatlichkeit konfrontiert, wobei das Dilemma der Gesetzherrschaft aus den folgenden vier schwierigen „Unverändertheiten“ immer besteht: Erstens bleiben die unausgewogene Internetentwicklung, unvollständige Regeln und schlechte Ordnung im globalen Cyberspace immer noch unverändert; zweitens bleibt die Grundsituation unverändert, in der die

17 Die technologischen Regeln bestehen aus Software, Protokollen, Programmen, Algorithmen, unterstützenden Einrichtungen und anderen technischen Elementen und sie bilden eine hybride technische Architektur. Im Wesentlichen handelt es sich dabei um eine Reihe von maschinenlesbaren Computercodes mit irreversiblen Ausführungseigenschaften. Die gesetzlichen Bestimmungen setzen sich aus rechtlichen Rahmenbedingungen, Bestimmungen, Industrierichtlinien usw. zusammen. Jeder Verstoß führt zu entsprechenden rechtlichen Haftungen.

Bedrohungen des Internets wie Verletzung der Privatsphäre, Verletzung der Rechte des geistigen Eigentums und Eindringung in Informationsressourcen weiter zunehmen. Drittens bleibt die Grundsituation unverändert, in der Cybersicherheitsvorfälle wie Schnüffler, Cyberangriffe und Cyberkriminalität nach wie vor sehr häufig sind. Und viertens sind die grundlegenden Umstände unverändert, unter denen noch häufige Gefahren in der Cyberwelt wie Cyberterrorismus, Cyberhegemonismus und Cybermilitarismus angegangen werden (Zhi Zhenfeng 2016). Einfach ausgedrückt, dass das globale Cyberspace-Verwaltungssystem mit ernsthaften, komplizierten und langwierigen Problemen behaftet ist und dass es an gesetzmäßiger Verwaltung mangelt und weitere Verwaltungstätigkeiten dringend erforderlich sind.

1. Ungleichgewicht im globalen Internetbetrieb und -management

Ebenso wie die reale Welt hängt die Cyberwelt von Verteilung und Verbrauch der Ressourcen für ihren Operationsbetrieb ab. IP-Adressen, Domännennamen, Ports, Protokolle und dergleichen sind erforderliche Kernressourcen für den Internetbetrieb. Diese Ressourcen können weder aus dem Nichts erzeugt noch nach Belieben verwendet werden, sondern sie müssen von spezialisierten Agenturen zugewiesen und verwaltet werden. Nach den verfügbaren Statistiken gehören zu den wichtigsten Internetbetriebs- und -verwaltungsorganisationen weltweit ICANN, RIRs, ISOC, IAB, IETF, IRTF, ISO, W₃C, INOG usw. (siehe Tabelle 5-11).¹⁸ Diese Organisationen bieten starke technische Unterstützung

18 Zu den Institutionen und Organisationen, die eine Rolle spielen und in gewissem Umfang am Betrieb des globalen Internets beteiligt sind, gehören: Asien-Pazifik Wirtschaftliche Zusammenarbeit (APEC), der Verband Südostasiatischer Nationen (ASEAN), der Europarat, die Europäische Union, Forum der Incident Response and Security Teams (FIRST), der Gruppe der Acht (G8), der Institution of Electrical and Electronics Engineers (IEEE), der International Telecommunication Union (ITU), Forum der Internetverwaltung (IGF) und der International Criminal Police Organization (INTERPOL), der Meridianprozess, die Organisation des Nordatlantikvertrags (NATO), die Organisation Amerikanischer Staaten (OAS), die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) usw.

für den globalen Betrieb des Internets an sich und verfügen über absolute Rechte auf Kontrolle und Dominanz. Als solche kontrollieren diese Organisationen fast alle Kernstandards und Schlüsselprotokolle in Bezug auf die Schlüsselinformationsinfrastruktur und die Kerntechnologien des Internets und bilden das „Rückgrat“ der globalen Cyberspace-Verwaltung. Aus der Mitgliedschaft dieser Institutionen, insbesondere ihrer Kernorgane, geht jedoch hervor, dass sie sich hauptsächlich in den Händen westlicher technologischer Mächte befinden, die von den Vereinigten Staaten geführt werden, und dies verspricht ein ernsthaftes Ungleichgewicht von der Wurzel an. Ein solches Ungleichgewicht führt dazu, dass einige Interessengruppen kein Rederecht oder keinen Einfluss auf das System haben. Dies zeigt sich insbesondere in zwei Aspekten: Erstens bestehen die Leitungsgremien und ihre Mitglieder hauptsächlich aus europäischen und amerikanischen Ländern oder ihren Bürgern, weshalb die Rechte und Interessen von Ländern mit unterentwickelten Internet-Technologien und ihren Bürgern nicht angemessen geschützt werden. Zweitens könnte die Autonomie der Entwicklungsländer bei der Wahl ihres eigenen Internet-Entwicklungsweges und ihres Internet-Verwaltungsmodells von dem Machtmonopol im globalen Cyberspace-Verwaltungssystem beeinträchtigt werden.

Tabelle 5-11 Wichtige globale Internetbetriebsorganisationen und ihre Verantwortlichkeiten

Organisation des Internetbetriebs	Hauptverantwortungen
Internet Corporation für zugewiesene Namen und Nummern (ICANN)	Verantwortlich für Koordinierung des einzigen Internet-Identifizierungssystems und dessen sicheren und stabilen Betrieb weltweit, einschließlich der räumlichen Zuweisung von Internetprotokolladressen, der Zuweisung von Protokollkennungen, der Verwaltung generischer Top-Level-Domain-Namen sowie nationaler und regionaler Top-Level-Domain-Namen Systeme und der Verwaltung von Root-Server-Systemen. Das Management-Team besteht aus ISOC-Mitgliedern; Mitarbeiter kommen aus vielen Ländern der Welt, die meisten aber aus den USA.
Regionale Internetregistrierungen (RIRs)	Sie sind dafür verantwortlich, digitale Internetressourcen in ihrer jeweiligen Region zuzuweisen und zu registrieren, die ICANN-Zuweisung vorzunehmen und den Volkswirtschaften IP-Adressen und AS-Nummern zuzuweisen. Mitglieder sind Internetorganisationen wie ISP und nationale (oder regionale) Internetregistrierungen (NIRs), bei denen es sich um gemeinnützige Mitgliedsorganisationen handelt.
Internet Society (ISOC)	Ziel ist es, vorteilhafte und offene Bedingungen für die weltweite Entwicklung des Internets zu schaffen, relevante Standards zu formulieren, Informationen zu veröffentlichen und Schulungen zur Internettechnologie durchzuführen. Darüber hinaus engagiert sich ISOC auch für soziale, wirtschaftliche, politische, moralische, legislative und andere Arbeiten, die sich auf die Entwicklungsrichtung des Internets auswirken. Die Direktoren gehören herausragenden Internet-Eliten aus der ganzen Welt an. Es ist eine nichtstaatliche, gemeinnützige, internationale Branchenorganisation mit Hauptsitz in den Vereinigten Staaten.

(Fortsetzung)

Tabelle 5-11 Fortsetzung

Organisation des Internetbetriebs	Hauptverantwortungen
Internet Architecture Committee (IAB)	Definiert die Struktur und legt langfristige Entwicklungspläne für den gesamten Cyberspace fest, führt die technische Überwachung und Koordination durch und ernennt und überwacht verschiedene internetbezogene Organisationen. Die Mitglieder werden von IETF-Teilnehmern gewählt und von ISOC-Direktoren ernannt. Insgesamt 15 professionelle Forscher aus verschiedenen Berufen auf der Welt. Das Komitee wurde 1979 vom US-Verteidigungsministerium und seiner Agentur für fortgeschrittene Forschungsprojekte gegründet und wurde 1992 dem ISOC angegliedert und dadurch von einer US-Regierungsbehörde zu einer internationalen öffentlichen Einrichtung geworden.
Internet Engineering Task Force (IETF)	Verantwortlich für Forschung, Entwicklung und Formulierung von technischen Spezifikationen im Zusammenhang mit dem Internet. Es wird spontan von Experten beteiligt und verwaltet und steht allen Interessierten der Branche offen. Die Organisation gehört zum ISOC und ist eine offene internationale Nichtregierungsorganisation.
Internet Research Task Force (IRTF)	Vom IAB autorisiert und verwaltet und verfügt über mehrere Gruppen, die theoretische Untersuchungen zu verschiedenen Fragen der Internet-Technologie durchführen.
Internationale Organisation für Normung (ISO)	Ziel ist es, Entwicklung der Normungsarbeit weltweit zu fördern, um den internationalen Materialaustausch und die gegenseitige Unterstützung zu erleichtern und Zusammenarbeit in den Bereichen Wissen, Wissenschaft, Technologie und Wirtschaft auszubauen. Die Hauptaufgabe besteht darin, internationale Standards zu formulieren, die Normungsarbeit weltweit zu koordinieren und mit anderen internationalen Organisationen zusammenzuarbeiten, um Normungsfragen zu untersuchen. Zu den Teilnehmern gehörten nationale Normungsgremien und große Unternehmen aus Mitgliedstaaten. Die höchste Autorität ist die ISO-Generalversammlung. Alle Mitglieder von ISO-Gruppen, Korrespondenten und internationalen Organisationen mit Verbindungen zur ISO sind auf der Versammlung vertreten. Es ist eine globale Nichtregierungsorganisation.

Tabelle 5-11 Fortsetzung

Organisation des Internetbetriebs	Hauptverantwortungen
World Wide Web Consortium (W3C)	Ziel ist es, relevante internationale Internetstandards zu untersuchen und zu erstellen, beispielsweise für offene Internetplattformen und drahtlose Internet-Technologien usw. Die Organisation wird von Tim Berners Lee, dem Vater des World Wide Web, und Jeffrey Jaffe, dem Chief Executive Officer, geleitet. Es wird gemeinsam von einem globalen Team betrieben, das an vier globalen Hauptsitzen von Massachusetts Institute of Technology, der Europäischen Union für Mathematik und Informatik, der Keio University in Japan und der Beijing University of Aeronautics and Astronautics in China angesiedelt ist. In der Natur handelt es sich um eine internationale neutrale Agentur für Technologiestandards, die als Projekt des CERN entwickelt wurde.
Internet Operators Alliance (INOG)	Erörtert und beeinflusst Fragen im Zusammenhang mit dem Betrieb des Internets. Zu seinen Mitgliedern zählen hauptsächlich Internetdiensteanbieter und Internet-Switch-Center usw.

Quelle: Siehe Zhi Zhenfeng: „Rechtsstaatlichkeit in der globalen Cyberspace-Verwaltung“, Recht und soziale Entwicklung, 1. Ausgabe, 2017

2. Cyber-Hegemonie und Cyber-Dominanz

Als Geburtsort des Internets haben die Vereinigten Staaten das Monopol auf die fortschrittlichsten Internet-Technologien und die wichtigste Internet-Infrastruktur der Welt, kontrollieren die Herstellung von wichtigen globalen Informationsprodukten und die Verwaltung von Internet-Adressressourcen und Root-Servern und haben das absolute Kontrollrecht, das andere Länder nicht haben können. Gleichzeitig befindet sich das Kontrollrecht der Cyberspace auch fast in der alleinigen Hand der Vereinigten Staaten. China und andere Länder befinden sich im Grunde genommen in der Grauzone der Cyberspace-Souveränität und halten tatsächlich nur „eine Hälfte“ von oder sogar „keine“ Cyberspace-Souveränität im Cyberspace, der sich in einem fast vollständigen Chaos befindet. Darüber hinaus folgen die

Vereinigten Staaten der „Doppelmoral“,¹⁹ befürworten den technologischen Liberalismus und schaffen eine technologische Diktatur, die dem Terrorismus und Militarismus eine Handhabe im Cyberspace bietet. „Obwohl die neue wissenschaftliche und technologische Revolution die nationale Souveränität aller Länder gleichermaßen untergräbt und einschränkt, betrifft dies die Industrie- und Entwicklungsländer in sehr unterschiedlichem Maße, was sehr unausgewogen und ungleich ist (Zhao Xudong 1997). Ein solches Ungleichgewicht und eine solche Ungleichheit sind tatsächlich Ausdruck der internationalen Beziehungen, in denen Alleinherrschaft und Knechtschaft unter der Cyber-Hegemonie Hauptrolle spielen. Dies untergräbt die internationale Gerechtigkeit erheblich und bringt die Länder der Dritten Welt in stark benachteiligte Positionen (siehe Tabelle 5-12).

Tabelle 5-12 Cyber-Hegemonie und Cyber-Dominanz

Form/Kategorie	Hauptmanifestation
Hegemonie im Cyber-Management	Einige westliche Industrieländer mit den Vereinigten Staaten an der Spitze haben das Monopol auf die Kernteile des Internets. Das Lebenselixier des Internets ist der Root-Server und das Domain-Name-System. Derzeit unterstützen weltweit 13 Root-Server den Betrieb des Internets, von denen sich der einzige primäre Root-Server und 9 der 12 sekundären Root-Server in den USA befinden, einer in Großbritannien und einer in Schweden und einer in Japan. Derzeit ist ICANN, das von der US-Regierung autorisiert und tatsächlich von den USA kontrolliert wird, für die einheitliche Verwaltung des globalen Internet-Root-Servers, des Domain-Name-Systems und des IP-Adressensystems verantwortlich. Das US-Handelsministerium hat jederzeit ein Veto gegen die Entscheidungen von ICANN und kann jederzeit in die Internet-Systeme anderer Länder eingreifen. Darüber hinaus dominieren einige westliche Industrieländer, die von den Vereinigten Staaten geführt werden, auch die Formulierung von Internetregeln.

19 „Doppelmoral“ bezieht sich auf die Anwendung unterschiedlicher Standards in Bezug auf Cyberfreiheit und -sicherheit, d.h. einen Standardsatz für sich selbst und seine Verbündete und einen anderen für Entwicklungsländer.

Tabelle 5-12 Fortsetzung

Form/Kategorie	Hauptmanifestation
Hegemonie der Cyber-Technologie	Die Vereinigten Staaten sind der Geburtsort der Computer- und Informationstechnologie. Die Amerikaner stellten den ersten elektronischen Computer der Welt her und schufen das erste Internet. Die USA sind anderen Ländern der Welt, einschließlich anderer westlicher Industrieländer, im IT-Bereich weit voraus. Die USA kontrollieren die Kerncomputer- und Internet-Technologien. Jedes wichtige Glied in der Internet-Industriekette wie Chips, Betriebssysteme und Suchmaschinen wird im Wesentlichen von amerikanischen Unternehmen dominiert. Unter ihnen sind Microsoft und Google offensichtliche Monopole in der Natur.
Sprachhegemonie und Monopol auf Netzwerkinformation sinhalte	Die Assemblersprache des Computers, das Betriebssystem sowie die Software- und Hardwarestandards sind alle in Englisch. Mehr als zwei Drittel des Informationsflusses im Internet stammen aus den USA, wobei Japan mit einem Anteil von nur 7 Prozent den zweiten Platz und Deutschland mit 5 Prozent den dritten Platz einnimmt. China hat nur 0,1 Prozent des Informationseingabeverkehrs und 0,05 Prozent des Ausgabeverkehrs des gesamten Internets. Es ist ersichtlich, dass Englisch die dominierende Sprache im Internet ist und die Industrieländer die „Hauptproduzenten“ von Informationen im Internet sind. Unter ihnen sind die USA die wichtigsten „Hersteller“ und wirklich der „Suzeränstaat der Netzwerkinformationen“.
Cyber- Ideologische Hegemonie	Einige westliche Industrieländer, angeführt von den USA, fördern und tünchen energisch westliche Wertanschauung wie „Freiheit“, „Demokratie“, „Menschenrechte“, „Gleichheit“, „Brüderlichkeit“ und „Gerechtigkeit“ im Internet. Sie befürworten westliche politische Modelle und betrachten das Internet seit Langem als wichtiges Instrument zur „Verbreitung der Demokratie“.

(Fortsetzung)

Tabelle 5-12 Fortsetzung

Form/Kategorie	Hauptmanifestation
	Der Cyber-Liberalismus ist zu einer der Hauptausreden für den Westen geworden, Cyber-Hegemonismus zu betreiben. Tatsächlich bedeutet der sogenannte „freie Informationsfluss im Cyberspace“, den die Vereinigten Staaten energisch fördern, „freien Fluss“ entsprechend den Bedürfnissen der Vereinigten Staaten.

Quelle: Siehe Wang Zhengping und Xu Tieguang: „Westlicher Cyber-Hegemonismus und Cyber-Rechte der Entwicklungsländer“, Thinking, 2. Ausgabe, 2011.

3. Cybersicherheit und Cyberkriminalität

Cybersicherheit und Cyberkriminalität sind ein weiteres schwieriges Problem der globalen Cyberspace-Verwaltung. Das Internet hat die natürliche Eigenschaft wie Virtualität, Anonymität, Grenzüberschreiten und Grenzlosigkeit, Offenheit und Zentrallosigkeit und Interaktionen in Echtzeit. Diese Eigenschaften bieten Kriminellen möglichen „Nährboden“, Straftaten wie Cyberangriffe, Cyberbetrug, Verkauf von Cyberpyramiden und andere kriminelle Aktivitäten anonym durchzuführen. Cybersicherheitsvorfälle und Cyberkriminalität treten von Zeit zu Zeit auf der ganzen Welt auf, und Bedrohungen wie Cyberterrorismus, Cyberhegemonismus und Cybermilitarismus sind zu allgemeinen Gefahren der Welt geworden. Im Allgemeinen gibt es zwei Arten von Cyberkriminalität. Die erste ist Hausfriedensbruch und Sabotage wie Schnüffler, Website-Angriffe und Verbreitung von Viren. Beispiele hierfür sind der „Snowden-Vorfall“, der „Fünf-Augen-Überwachungsvorfall“, Stuxnet usw. Die zweite Art sind im Internet begangene traditionelle Verbrechen wie Online-Finanzbetrug, illegale Internetfinanzierung, Cyberdiebstahl usw. Andere Formen traditioneller Verbrechen wie Falsche Werbung, Cyber-Fahndung, Beleidigung und Diffamierung sowie Online-Spionage haben schwerwiegende Auswirkungen auf das bestehende globale Sicherheitssystem. Im Vergleich zu traditionellen Verbrechen weisen Cyberkriminalität drei

offensichtliche Merkmale auf: Erstens sind sie tendenziell destruktiver und werden immer mehr von jüngeren Tätern begangen. Zweitens sind die Kosten für solche Verbrechen zu niedrig, aber die Zahl der Opfer kann sehr groß und die wirtschaftlichen Verluste können sehr hoch sein. Drittens kann der Schaden weit verbreitet sein, der alle Branchen und Bereiche betreffen, während einige sogar die politische, wirtschaftliche und soziale Sicherheit bedrohen sowie die Stabilität der Länder auf dem Spiel stellen können.

(III) Datenrechte als Lösung für die globale Internetverwaltung

Die Rechtsstaatlichkeit ist ein wichtiges Mittel der globalen Cyberspace-Verwaltung. Der Kern der Rechtsstaatlichkeit ist das Gesetz. „Das Gesetz stammt aus der menschlichen Natur. Es wird vom Volk geschaffen und existiert für das Volk. Es beginnt mit dem Volk und endet im Dienste des Volkes“ (Qin Ying 2009). Mit dem Ziel der globalen Internetverwaltung gehen wir von der grundlegenden Theorie der Hypothesen der Menschlichkeit aus und versuchen, das Problem mit der Hypothese des „Datenmenschen“ anzugehen. „Rechte, die von „Datenmenschen“ abgeleitet sind, werden als Datenrechte bezeichnet. Auf der Grundlage von Datenrechten erstellte Ordnung wird als Datenrechtssystem genannt. Und die auf der Basis des Datenrechtssystems auf diese Weise zustande gekommenen Rechtsnormen werden als Datenrechtsgesetz bezeichnet. Damit kommt der gesetzliche Rahmen für ‚Datenrecht-Datenrechtssystem-Datenrechtsgesetz‘“ zustande (Schlüssellabor der Big-Data-Strategie 2018).

1. Datenrecht, Datenrechtssystem und Datenrechtsgesetz

Das Datenrechtsgesetz ist eine Rechtsnorm, die auf der Basis des Datenrechtssystems entsteht. Dabei handelt es sich um neue Verteilung und rationale Optimierung von Verantwortlichkeiten, Rechten und Pflichten, um verschiedene Beziehungen und Interessenkonflikte zu regulieren, die im Cyberspace auftreten. Anders als traditionelle

Gesetze wie Zivilrecht, Handelsrecht, Strafrecht, Verwaltungsrecht und Sachenrechtsgesetz regelt das Datenrechtsgesetz in Bezug auf Regulierungsobjekte und -umfang neue Arten von sozialen Beziehungen und Rechtsverpflichtungsverhältnissen im Cyberspace mit Daten als Mittelpunkt. Da Daten eine breite Abdeckung haben und die Regulierung von Daten über verschiedene Grenzen hinweg erfolgen kann, kann das Datenrechtsgesetz Inhalte enthalten, die von Natur aus im Zivil-, Verwaltungs- und Strafrecht zu sehen sind und mehrere Kategorien von Rechtsbeziehungen umfassen. Das heißt, dass die Objekte der Regulierung weit verbreitet sind und dass der Umfang der Regulierung grenzüberschreitend ist. Das Datenrechtsgesetz ist eine Sammlung von Rechtsnormen, die verschiedene Rechtsverpflichtungsbeziehungen im Cyberspace regeln. Der Kern davon ist die Regelung des Dateneigentums, der Datenrechte, der Datennutzung und des Datenschutzes. Beispielsweise wirken sich die neuen Arten von gesetzlichen Rechten, die im Cyberspace derivativ entstanden sind, wie z. B. das Dateneigentumsrecht, Datenpersönlichkeitsrecht, Teilhaberecht auf Daten und Recht auf Vergessen von Daten, ständig auf die traditionellen rechtlichen Definitionen der Menschenrechte, Sachenrechte und Rechte an geistigem Eigentum aus und lösen Änderungen in den Funktionsmechanismen traditioneller Rechtssysteme in Bezug auf Finanz, Handel, Vertrag, Gerichtsverfahren usw. aus. Trotz alledem ist das Datenrechtsgesetz für den ordnungsgemäßen Datenfluss im Cyberspace notwendig, das ist eine Voraussetzung für die Wiederverwendung von Daten und stellt ein Gleichgewicht zwischen Datenschutz und Datennutzung sowie eine grundlegende Komponente für den Bau der „quadratischen Welt“ des Rechtsimperiums im Cyberspace dar.

2. Datenrechtsgesetz als Lösung der globalen staatsrechtlichen Internetverwaltung

Der Cyberspace ist kein „Ort außerhalb des Gesetzes“. Die internationale Gemeinschaft braucht ein faires und gerechtes System der rechtsbasierten Cyberspace-Verwaltung. Seit der offiziellen Verbindung mit dem Internet 1994 hat China die Internet-Rechtsstaatlichkeit die Stufen 1.0, 2.0 und 3.0

durchlaufen (siehe Tabelle 5-13). In der 3.0-Phase entwickelte sich der globale Internet-Branche boomend wie nie zuvor, aber es gab auch zahlreiche Risiken und stetige Bedrohungen, deren Regulierung ein gerechteres und zukunftsorientiertes Rechtssystem erfordert. Das Datenrechtsgesetz wurde gerade dann ins Leben gerufen, als es ein zentraler Bestandteil und wichtiger Kerninhalt der Internet-Rechtsstaatlichkeit 3.0 sein sollte. Es konzentrierte sich auf die wichtigsten Fragen der Rechtsstaatlichkeit im Cyberspace wie Datenteilhabe, Datensicherheit, Datenrechtsschutz und Datenhoheit etc. Der letztendliche Zweck des Datenrechtsgesetzes besteht darin, Regeln, Disziplin und Grundlinie für den Cyberspace und die Cybergesellschaft festzulegen. Es ist die gesetzliche Norm, die verschiedenen Beziehungen und Interessenkonflikte im Cyberspace regelt und wichtige Unterstützung für Wahrung der Cyberspace-Souveränität und Förderung von Innovationen in der Internetbranche sowie für relevante technologische Innovationen und Geschäftsmodelle bietet. Wenn das Sachenrechtsgesetz im Zeitalter der industriellen Zivilisation ein natürlicher Muss ist, ist das Datenrechtsgesetz im Zeitalter von Big Data ein wesentlicher Muss für die Rechtsstaatlichkeit im Cyberspace. Es handelt sich dabei um den Grundrahmen für die Rechtsordnung im Cyberspace, repräsentiert die gesetzbasierte Cyberspace-Verwaltung durch den Staat und bietet wichtige Unterstützung und eine gesetzbasierte Lösung für die globale Internet-Verwaltung.

Tabelle 5-13 Internet-Rechtsstaatlichkeit 1.0, 2.0 und 3.0

Zeitphase	Eigenschaften
Internet Rule of Law 1.0 (1994–2000)	Das Internet übertrug hauptsächlich Informationen, die meist in statischer Form vorliegen. Die Art der Informationsübertragung war relativ einfach. Das Internet hatte keinen tief greifenden Einfluss auf Gesellschaft, Wirtschaft und Leben. Daher konzentrierte sich die Internet-Rechtsstaatlichkeit in dieser Phase hauptsächlich auf Steuerung der Internetinfrastruktur, einschließlich der Verwaltung von IP-Adressen, der Verwaltung von Domännennamen und der Sicherheitsverwaltung von Computerinformationssystemen.
Internet Rule of Law 2.0 (2000–2013)	Das Internet übertrug hauptsächlich Wert. E-Commerce, soziale Medien und Suchmaschinen wurden zu den drei Säulen des Internets. Der Informationsfluss wandelte sich allmählich in einen Wertefluss um. Benutzer wurden zum Kern der Internetdienste. Zu diesem Zeitpunkt bestand die Rechtsstaatlichkeit im Internet hauptsächlich aus der Verwaltung der Internetbranche, Internetinformationsdiensten, dem klassifizierten Schutz der Sicherheit und der Verwaltung von Online-Transaktionen.
Internet Rule of Law 3.0 (2013-jetzt)	Der Cyberspace erlebt ein Chaos, da er sich zu schnell entwickelt und dringend eine gute Ordnung benötigt. In dieser Phase haben sich mit dem raschen Aufstieg der Informationstechnologien der neuen Generation wie Big Data, künstliche Intelligenz und Blockketten die Informationsökonomie, die Cyberökonomie und digitale Ökonomie zu neuen Wirtschaftsformen etabliert. Gleichzeitig sind die negativen Auswirkungen wie Verlust persönlicher Informationen, des grenzüberschreitenden Datenflusses und des Cyberterrorismus aufgetreten und haben Alarm geschlagen. Internetprobleme wie Cybersicherheit, Datensicherheit und Schutz der Datenrechte müssen gesetzlich geregelt werden.

3. Datenrechtsgesetz: Anstoß zum Aufbau einer Schicksalsgemeinschaft im Cyberspace

Der Aufbau einer „Schicksalsgemeinschaft im Cyberspace“ ist eine schöne Vision für die Entwicklung des Cyberspace und auch eine wichtige Garantie dafür, dass das Internet der Menschheit mehr Vorteile bringen kann. Als Regelsystem, das auf der Basis menschlicher Rationalität geschaffen

wird, existieren die Rechtssysteme immer in bestimmter Zeitspanne und bestimmten Räumen (Huang Zhirong 2017). Seit dem Eintritt in die Ära von Big Data hat China seine Bemühungen um Forschung über und Einrichtung von Datenrechten, des Datenrechtssystems und des Datenrechtsgesetzes nie eingestellt. Mit dem Datenrechtsgesetz als übergeordnetem Projekt haben wir erste Erfolge beim Aufbau der Rechtsstaatlichkeit im Internet erzielt und ein Muster aus gutem Recht und guter Regierungsführung gebildet.²⁰ Als Entscheidungsform der Zuweisung von Rechten und Pflichten in Bezug auf Ressourcen im Cyberspace verkörpert das Datenrechtsgesetz die Ideologie, Wertanschauung und Philosophie des Internetzeitalters. Die digitale Zivilisation ist die Wertbegründung und treibende Kraft für Reform und Innovation des Datenrechtsgesetzes, wobei das Datenrechtsgesetz auch Grundlage für die Existenz der digitalen Zivilisation bietet, zur Aufrechterhaltung ihrer Systeme und zur Verbesserung ihrer Ordnung beiträgt. Insofern konzentriert sich die Kernbedeutung des Datenrechtsgesetzes auf dem Ordnungsparadigma der digitalen Zivilisation und bildet die Grundlage für Aufrechterhaltung der Ordnung in dieser Zivilisation (Schlüssellabor der Big-Data-Strategie 2018). In diesem Sinne ist das Datenrechtsgesetz das Produkt eines Sprunges unserer Zivilisation und die Rechtsgrundlage für den Aufbau einer Schicksalsgemeinschaft der Menschheit im Cyberspace. Zusammen mit dem Gesetz der dinglichen Rechte bildet es zwei rechtlichen Grundlagen für die Ära der digitalen Zivilisation, die den Sprung der menschlichen Welt von der industriellen Zivilisation zur digitalen Zivilisation vorantreibt.

20 Die Entwicklung der Internet-Rechtsstaatlichkeit, deren übergeordnetes Projekt das Datenrechtsgesetz ist, hat eine doppelte Struktur mit speziellen Gesetzen für den Cyberraum und traditionellen Gesetzen, die im Cyberspace weiterhin angewendet werden. Dieses Rechtssystem umfasst Gesetze zum Schutz der wichtigsten Internetinfrastruktur, zur Überwachung der Internetbranche und zur Verwaltung von Internetinhalten und Internetverbrechen sowie internetorientierte juristische Auslegungen. Es deckt alle wichtigen Bereiche und Schlüssel-Kettenglieder des Cyberspace ab und verfügt über eine Hierarchie von Gesetzen, Vorschriften, Regeln und anderen Rechtsinstrumenten. Alle Rechtsregeln in diesem Struktursystem basieren auf regulativen Rechtsquellen, alle Regeln sind kodifiziert geschrieben und das System gehört zum Bereich des öffentlichen Rechts.

Literaturverzeichnis

- Das Nationale technische Komitee für Standardisierung der Informationssicherheit und Sonderarbeitsgruppe für Big-Data-Sicherheitsstandards: „Weißbuch zur Standardisierung der Big-Data-Sicherheit (Version 2017)“, <<http://www.cesi.cn/uploads/soft/170411/1-1F411162633.pdf>>, 11. April 2017
- Dong Lisheng „Eine institutionelle Analyse der Entwicklung von E-Verwaltung in der Europäischen Union“, in Zeitschrift der Parteischule des Stadtausschusses der CPC Hangzhou, 5/2012.
- E-Regierungsführung-Forschungszentrum der Parteischule des Zentralkomitees der KP Chinas (Nationale Verwaltungsakademie): Bericht über Entwicklung der digitalen Regierung, <http://www.egovernment.gov.cn/art/2019/8/2/art_194_6195.html>, 02. August 2019
- Hai Qun u. Wu Rina: „E-Regierungsführungs-Strategie in Japans i-Japan-Strategie 2015“, in Bürogeschäftsdienst, 4/2010.
- He Xinghui: „Chinas erstes lokales Gesetz zum Schutz der Big-Data-Sicherheit wurde formal umgesetzt und Guizhou Big-Data-Industrie genießt ein effektiveres und effizienteres Management und nicht mehr ‚Jeder auf seine Weise‘“, Tageszeitung der Wissenschaft und Technologie, 14. Oktober 2019.
- Huang Zhirong: „Forschung über Chinas Internet-Gesetzgebung“, Parteihochschule des Zentralkomitees der KP Chinas, Doktorarbeit, 2017.
- Legislative Arbeitskommission des Ständigen Ausschusses des Volkskongresses der Provinz Guizhou: „Auslegung der Vorschriften zur Big-Data-Sicherheit der Provinz Guizhou“, Guizhou Tageszeitung, 26. September 2019.
- Li Aijun: „Attribut und gesetzliche Eigenschaft des Datenrechts“, in Orientalisches Recht, 3/2018.
- Li Aijun: „China Big Data-Bericht zur Entwicklung der Rechtsstaatlichkeit“, Rechtsverlag, 2018.
- Li Wei: „Erfolg und Bedauern - Erstellung der Verfassung von Japan nach dem zweiten Weltkrieg“, in „Buchlesen“, 4/2009.
- Lian Cheng, Yang Fei u. Zhang Hengye: „Bewertung der Entwicklung der E-Regierungsführung in Südkorea und Japan“, in Management Observer, 19/2018.
- Lian Yuming: „Big Data Blaues Buch: China Big-Data-Entwicklungsbericht Nr. 1“, Sozialwissenschaftliche akademische Presse, 2019.
- Liu Yeting u. Tang Sisi: „Auswirkungen und Herausforderungen von Big Data auf die Regierungsführung“, in E-Regierungsführung, 6/2014.
- Liu Ziheng u. Zhou Jiagui: „u-JAPAN-Plan und sein Entwicklungsstand in Japan“, in Journal der Universitätsbibliothek, 3/2013.

- Nobuyoshi Ashibe: „Verfassung“, 3. Version, übersetzt von Lin Laifan et al., Peking University Press, 2006.
- Qi Aimin u. Pan Jia: „Forschung über rechtlichen Unterstützungsmechanismus für Big-Data-Sicherheit“, in Zeitschrift der Chongqing Universität für Post und Telekommunikation (Sozialwissenschaft Edition), 3/2015.
- Qin Ying: „Das Gesetz aus der Hypothese der bösen menschlichen Natur verstehen“, in Theoretische Beobachtung, 3/2009.
- Ran Congjing: „Spezialthema: Netz- und Datensouveränität jenseits geografischer Grenzen“, in „Journal der Informationsressourcenverwaltung“, 2/2019.
- Ran Congjing & Wang Bingjie: „Forschung über Modell der internationalen Strategie zur Internet-Hoheitssicherheit“, in „Journal der Informationsressourcenverwaltung“, 2/2019.
- Wang Tze-chien: „Thema und Ausblick des Schutzes des Persönlichkeitsrechts(III) - das Recht der Privatsphäre“, (Band I), in „Regionale Rechtskunde in Taiwan“, 96/2007.
- Wang Zhengping und Xu Tiegung: „Westlicher Cyber Hegemonismus und Cyber-Rechte der Entwicklungsländer“, Thinking, 2. Ausgabe, 2011.
- Schlüssellabor der Big Data-Strategie: „Datenrechtsgesetz 1.0: Theoretische Basis des Datenrechts“, Verlag der sozialwissenschaftlichen Literatur, 2018, Worte des Chefredakteurs.
- Wei Jianxin u. Song Renchao: „Erfahrung und Referenz der Gesetzgebung zum Schutz persönlicher Rechte in Japan“, in Zeitschrift der Shenyang Universität der Technologie (Sozialwissenschaften), 4/2018.
- Wu Shan: „Li Keqiang unterzeichnet Dekret des Staatsrates zur Verkündung überarbeiteter Vorschriften der Volksrepublik China über offene Regierungsinformationen“, in Volkszeitung. 16. April 2019.
- Xie Qing: „Das Rechtssystem des Schutzes personenbezogener Daten in Japan und seine Aufklärung“, in „Zeitschrift für Politik und Recht“, 6/2006.
- Yao Guozhang u. Lin Ping: „Planung und Bereitstellung von E-Regierungsführung und E-Regierungs-Entwicklung in Japan“, in E-Regierungsführung, 12/2009.
- Yao Yuerong: „Schutz personenbezogener Daten aus Sicht der Verfassung“, Doktorarbeit an der Ostchinesischen Universität für Politikwissenschaft und Rechtskunde, 2011.
- Zhao Xudong: „Der Einfluss der neuen technologischen Revolution auf die nationale Souveränität“, in „Europa“, 6/1997.
- Zhao Yanqiu: „Aufbau eines Schutzmodells für Recht auf Cyberprivatsphäre“, in „Journal Suche nach Wahrheit“, 3/2005.
- Zhao Yingying: „Mehrere NPC-Abgeordnete schlagen vor, die Gesetzgebung zur Datensicherheit zu beschleunigen und Daten des öffentlichen Verkehrs usw.

unter der Voraussetzung des Datenschutzes zuerst bereitzustellen“ Peking Abendzeitung, 7. März 2019.

Zhi Zhenfeng: „Globale Vision der Schicksalsgemeinschaft im Cyberspace und Chinas Verantwortung“, in Guangming Tageszeitung, 27. November 2016.

Zhi Zhenfeng: „Rechtsstaatlichkeit in der globalen Cyberspace-Verwaltung“, in Recht und soziale Entwicklung, 1/2017.

Zhong Guangping: „Mitglied des Nationalen CPPCC-Komitees Lian Yuming: Ein Vorschlag zur Beschleunigung der Gesetzgebung zur Datensicherheit“, in Chinas Radio und Fernsehen, 6/2018.

Zhou Hanhua: „Anmerkungen zu einigen Fragen im Zusammenhang mit dem Gesetz zum Schutz personenbezogener Daten (Entwurfsversion basierend auf Empfehlungen von Experten)“, in Chinas Jahrbuch des Wissenschafts- und Technologierechts, 1/2005.

„Vorschriften der Stadt Guiyang über Big-Data-Sicherheitsverwaltung“, in Guiyang Daily, 16. August 2018.

Nachwort

Der Begriff „Datenrechtsgesetz“ wurde vom Professor Lian Yuming, Direktor des Schlüssellabors für Big-Data-Strategie, im März 2017 erstmals vorgeschlagen und dann vom Nationalen Komitee für Begriffe in Wissenschaften und Technologien in China offiziell anerkannt. Im Juli 2017 wurde das Forschungszentrum für Datenrechtsgesetz der chinesischen Universität für Politikwissenschaft und Recht mit Professor Lian Yuming als Direktor offiziell gegründet. Das ist die erste Forschungseinrichtung für Datenrechtsgesetz in China.

Am 28. Mai 2019 beriefen die Chinesische Universität für Politikwissenschaft und Rechtskunde und die Volksregierung der Stadt Guiyang gemeinsam das Eröffnungsmeeting der Digital China Think Tank Alliance und das Symposium zum Datenrechtsgesetz 1.0 (vereinfachte und traditionelle chinesische Version und englische Version) ein. Zhao Deming, Mitglied des Ständigen Ausschusses des CPC Guizhou Provincial Committee und Sekretär des CPC Guiyang Municipal Committee, nahm an der Sitzung teil und hielt eine Rede. Er lobte das Datenrechtsgesetz 1.0 als ein großer Erfolg der theoretischen Innovation. Das Datenrechtsgesetz 1.0 hat gleich nach seiner Veröffentlichung weltweit große Aufmerksamkeit auf sich gezogen. Es wurde von mehr als 170 chinesischen und über 200 ausländischen Medienagenturen in Englisch, Französisch, Deutsch und Spanisch sowie in Chinesisch berichtet. Eine ausländische Medienagentur kommentierte: „Seine Veröffentlichung bietet eine juristische Grundlage für die Transformation der menschlichen Gesellschaft von der industriellen Zivilisation zur digitalen Zivilisation und gibt uns einen neuen Schlüssel für die Zukunft der digitalen Zivilisation.“ Die Veröffentlichung des Datenrechtsgesetzes 1.0 markierte den Eintritt chinesischer Gesetze auf die Weltbühne. Es ist auch ein wirksames und wichtiges Rechtsinstrument für die Beteiligung Chinas an der globalen Verwaltung.

Das „Datenrechtsgesetz 1.0“ enthüllt die theoretische Logik, Werte-logik und Rechtslogik von Datenrechten und erörtert zehn grundlegende

Gesichtspunkte: a. Menschenrechte, Sachenrechte und Datenrechte sind drei Kategorien von Grundrechten der Menschheit in der Zukunft; b. Datenrechte sind eine Kombination aus Persönlichkeitsrechten und Eigentumsrechten; c. Subjekte der Datenrechte sind bestimmte Rechtsinhaber, während Objekte bestimmte Datensätze sind; d. Datenrechte durchbrechen die Beschränkungen von „ein Recht für ein Objekt“ und „Dinge sind greifbar“ und werden häufig als „mehrere Besitzrechte für eine Daten“ manifestiert; e. Das Datenrecht hat die Eigenschaft der Privatrechte, öffentlicher Rechte und souveräner Rechte; f. Das Datenrechtssystem hat fünf grundlegende Dimensionen: das System der Legalisierung von Datenrechten, das Dateneigentumssystem, das System der Nießbrauchrechte auf Daten, das System der Gemeinnutzrechte auf öffentliche Daten und das Datenteilhabesystem; g. Das Teilhaberecht ist das Wesen der Datenrechte. h. Das Datenrechtsgesetz enthält gesetzliche Normen, die das Dateneigentumsrecht, Datenrecht, Datennutzung und Datenschutz regeln. i. Das Datenrechtsgesetz rekonstruiert die digitale Zivilisation. j. Das Datenrechtsgesetz ist ein wichtiger Schritt auf dem Weg von der industriellen zur digitalen Zivilisation. Das ist der Ausgangspunkt für uns, um das Datenrechtsgesetz zu verstehen und zu studieren.

Das Datenrechtsgesetz 2.0 ist Fortsetzung und Vertiefung des Datenrechtsgesetzes 1.0. Erstens wurde der Begriff der „Datenmensch-Hypothese“ erstmals vorgeschlagen, was auch als logischer Ausgangspunkt für Studien zum Datenrechtsgesetz gilt, dessen Kern der Altruismus ist. Zweitens werden drei Hauptrechte im Zeitalter von Big Data im Zusammenhang mit Datenrechten vorgeschlagen, nämlich das Datenrecht, Teilhaberecht und die Datenhoheit. Drittens ist es eine Antwort auf die wichtigen Anweisungen von Präsident Xi Jinping in seinem Glückwunschs Schreiben an die China International Big Data Industry Expo 2019, dass wir „die Herausforderungen bei der Entwicklung von Big Data in den Bereichen Gesetz, Sicherheit und Regierungsverwaltung bewältigen sollten“. Dieses Buch basiert fest auf Diskussionen und Austausch sowie auf eingehenden Forschungsanstrengungen, die vom Schlüssellabor für Big-Data-Strategie organisiert wurden und wurde von allen Autoren in Zusammenarbeit verfasst. Die Kernideen und die allgemeine Struktur des Buches stammen von Lian Yuming und das totale Design der Rahmenstruktur wurde

auch von ihm gemacht, während eine detailliertere Gliederung sowie die wichtigsten Punkte hauptsächlich von Long Rongyuan und Zhang Longxiang ausgearbeitet wurden. Zu den Autoren gehören Lian Yuming, Zhu Yinghui, Song Qing, Wu Jianzhong, Zhang Tao, Song Xixian, Long Rongyuan, Zhang Longxiang, Zou Tao, Shen Xudong, Chen Wei, Yang Guanhua, Yang Lu und Yang Zhou sowie Long Rongyuan als Koordinator. Chen Gang bot viele wichtige zukunftsweisende und wegweisende Ideen für dieses Buch. Bedeutende und zukunftsweisende Beiträge kamen auch von Zhao Deming, Mitglied des Ständigen Ausschusses des CPC Guizhou Provincial Committee und Sekretär des CPC Guiyang Municipal Committee; Yan Aoshuang, stellvertretender Vorsitzender des Ständigen Ausschusses des Beijinger Stadtvollkongresses und Direktor des Beijinger Stadtkomitees der Zhigong-Partei; Chen Yan, stellvertretender Sekretär des CPC Guiyang Municipal Committee und Bürgermeister von Guiyang; Xu Hao, Mitglied des Ständigen Ausschusses des CPC Guiyang Municipal Committee und Executiver stellvertretender Bürgermeister von Guiyang; Liu Benli, Mitglied des Ständigen Ausschusses und Generalsekretär des CPC Guiyang Municipal Committee; und Professor Li Zheng, Generalsekretär des Akademischen Komitees und Dekan des Instituts für künstliche Intelligenz und Rechtsstaatlichkeit der chinesischen Universität für Politikwissenschaft und Rechtskunde. Besonderer Dank geht an die Leiter und Herausgeber der Sozialwissenschaftsakademie Press. Sein Präsident Xie Shouguang sprach mit seinen tiefen Einsichten, seiner einzigartigen Vision und seinem großen Mut hoch über das Buch und bot Unterstützung für seine Veröffentlichung. Er organisierte eine Gruppe hochkarätiger Redakteure, um sorgfältige Pläne zu schmieden, gewissenhaft an der Bearbeitung zu arbeiten und ein ausgezeichnetes Design für das Buch zu präsentieren. Ohne diese wäre das Buch nicht wie geplant erschienen.

Während unserer Recherche und Zusammenstellung dieses Buches wurden mehrere hochrangige akademische Seminare abgehalten. Über 30 Experten und Gelehrten aus den Bereichen Recht, Wissenschaft und Übersetzung hatten mehrere Diskussionsrunden. Sie sind Wu Dahua, Liu Hongyu, Qu Qingchao, Kong Qingjiang, Xie Quan, Zhang Qing, Zhou Xuefeng, Tian Linan, Li Youxing, Ma Jing, Zhang Jiyu, Zhu Yinghui, Lied Qing, Zhang Zhuhong, Pan Shanbin, Sun Zhiyu, Qi Jun, Xu Yan, Zhu

Xiaowu, Wang Hao, Xiao Yu, Fu Yao, Wang Liping, Zhang Biao, Gao Xiangyu, Dai Jiajia, Zhang Chunyang, Wang Jing, Wu Yueguan und Zhu Jingjie. Unter diesen Experten sind Wu Dahua (Akademie der Sozialwissenschaften Guizhou), Xie Quan (Universität Guizhou), Pan Shanbin (Nationalitätsuniversität Guizhou), Wang Hao (Guizhou Xiaoi Robot Technology Co., Ltd.), Xiao Yu (ZhongChuangLian Anwaltskanzlei Guizhou) und Wang Jing (Guiyang Global Big Data Exchange) der Ansicht, dass mit dem Fortschritt von Wissenschaft und Technologie auch die Gesetze mit der Zeit Schritt halten müssen, dass wir angesichts verschiedener neuer Dinge, die nacheinander herauskommen, inklusiv und aufgeschlossen sein sollen und dass das Konzept des „Datenrechtsgesetzes“ rechtsgültig und zukunftsweisend ist. Zhang Jiyu (Renmin Universität von China), Zhu Xiaowu (Chinesische Universität für Politikwissenschaft und Rechtskunde), Sun Zhiyu (Guizhou Universität) und Xu Yan (Chinesische Universität für Politikwissenschaft und Rechtskunde) wiesen darauf hin, dass die Vorschläge für „Datenmensch“ und „Teilhaberecht“ notwendig und vorausschauend sind, dass die Hypothese des „Datenmenschen“ die Vision der Rechtsgemeinschaft erweiterte, während das Teilhaberecht große Bedeutung für die Koordinierung und das Gleichgewicht zwischen den privaten Rechten und der öffentlichen Macht auf Daten hat. Viele Experten wie Liu Hongyu (Jincheng Tongda & Neal), Qu Qingchao (Langes Dateninstitut), Kong Qingjiang (Chinesische Universität für Politikwissenschaft und Rechtskunde), Zhou Xuefeng (Universität für Luft- und Raumfahrt Beijing) und Li Youxing (Zhejiang Universität) glauben, dass das „Datenrechtsgesetz“ als das im chinesischen Diskurs vorgebrachte Pionierkonzept einen neuen Durchbruch in der rechtstheoretischen Forschung zu Big Data in China und der Welt markierte. Zhu Yinghui (Internationales Institut für Stadtentwicklung Peking) und Song Qing (Guiyang-Institut für innovationsgetriebene Entwicklungsstrategie) sind der Meinung, dass die Forschung zum Datenrechtsgesetz tatsächlich Untersuchung der Entwicklungstrends von Technologie, Recht und menschlicher Gesellschaft bedeutet; dass das Datenrechtsgesetz eine moderne Lösung für Untersuchung technologiebasierter Verwaltung und Verwaltungskapazität im Zeitalter der Wiedervermischung darstellt; dass es orientalische Weisheit bot, an unserem Recht festzuhalten, Regeln für Datenrechte zu formulieren

und unsere Stimme in der internationalen Gemeinschaft hören zu lassen; und dass wir uns so über zukünftige Rechtssysteme aus der Perspektive der menschlichen Zivilisation rational denken. Die Übersetzungsexperten Zhang Qing, Tian Linan, Ma Jing, Qi Jun, Fu Yao, Wang Liping, Dai Jiajia und Zhang Chunyang von der chinesischen Universität für Politikwissenschaft und Rechtskunde erklärten, dass das Datenrechtsgesetz ein Thema innovativer und interdisziplinärer Forschung ist, was kreativ, attraktiv und einflussreich ist; dass die Übersetzung dieser Buchreihe zum Datenrechtsgesetz in mehreren Sprachen ein wichtiges Fenster für den Dialog zwischen chinesischen und ausländischen Rechtsexperten darstellt; und dass es die Vision der globalen Datenrechtsstudie weltweit erheblich erweitert und ein neues Kapitel in der globalen Datenrechtsstudie aufgeschlagen hat.

Die vom Schlüssellabor für Big-Data-Strategie herausgegebenen „drei Buchreihen“ über digitale Zivilisation: „Blockdaten“, „Datenrechtsgesetz“ und „Souveränitäts-Blockketten“ sind neue Meilensteine in der Entwicklung von Big-Data-Theorien und als drei Hauptpfeiler der Rekonstruktion neuer Ordnung der digitalen Zivilisation bekannt. Sie haben relativ großen Einfluss im In- und Ausland. Unsere Gesetze stehen niemals wie jetzt vor großen Herausforderungen als die, die die heutige Entwicklung von Wissenschaft und Technologie mit sich bringt. Wir sollen den neuesten Technologien große Aufmerksamkeit widmen und aktiv auf diese Herausforderungen reagieren, mögliche Risiken kontrollieren, ein Gleichgewicht zwischen der Entwicklung von Recht und Wissenschaft herstellen und die Transformation zwischen Gesetzen, Rechtsstaatlichkeit und Rechtstheorie als Reaktion auf den sozialen Wandel aktiv fördern. Der Vorschlag für Datenrechtsgesetz hat Beitrag dazu geleistet, eine rechtliche Grundlage für Wahrung der nationalen Datenhoheit zu schaffen, das Recht für Formulierung von Regeln und unsere Stimme in Bezug auf Datenrecht in der internationalen Gemeinschaft hören zu lassen sowie das Recht für die Förderung der Rechtsstaatlichkeit in der globalen Cyberspace-Verwaltung in unseren Händen zu halten. Er ist für den Aufbau einer Schicksalsgemeinschaft im Cyberspace von besonderer Bedeutung. Die Forschung zum Datenrechtsgesetz ist eine bahnbrechende theoretische Untersuchung, die sich sowohl an der Gegenwart als auch an der Zukunft orientiert. Sie wird sich definitiv auf die Entwicklung der digitalen Wirtschaft, der digitalen

Regierung, die Verwaltung der digitalen Gesellschaft und den Fortschritt der digitalen Zivilisation positiv auswirken. Wir werden unsere Arbeit fortsetzen und das „Datenrechtsgesetz 3.0: Die gesetzgeberische Vorausschau“, das „Datenrechtsgesetz 4.0: Teilhaberecht und Recht auf Privatsphäre“ sowie das „Datenrechtsgesetz 5.0: Datenrechtstheorie und neue Ethik“ erstellen, um das theoretische System des Datenrechtsgesetzes weiter auszubauen und zu vervollständigen.

Während des Schreibens und Redigierens dieses Buches haben wir unser Bestes getan, Informationen über die neuesten Studien zu sammeln und die neuesten Ideen aufzunehmen. Da dieses Buch jedoch verschiedene komplizierte Bereiche abdeckt, wird es immer Einschränkungen geben und unser Verständnis ist möglicherweise nicht ganz korrekt. Für mögliche Fehler und insbesondere das Auslassen von Zitaten im Buch entschuldigen wir uns und freuen uns über Kommentare aller Leser. Die erste Dampfmaschine der Welt konnte nicht benutzt werden und das erste Auto konnte auch nicht wirklich auf die Straße fahren. Was neu ist, ist definitiv unvollkommen. Wir glauben jedoch daran, dass „es am möglichsten Gesetze sind, die sich auf die digitale Wirtschaft beziehen, wenn die chinesischen Gesetze die Weltbühne besteigen sollen“. In dieser Hinsicht machen wir unermüdlich große Anstrengungen, obwohl diese Sache sehr schwierig ist, sind wir voller Zuversicht und glauben, dass wir große Möglichkeiten haben und unsere Fähigkeiten voll zur Geltung kommen können.

Schlüssellabor für Big-Data-Strategie
Beijing, den 16. Januar 2020

Nomenklatur

- Abgeflacht 32
- Absichtsrecht 71
- Absolute Macht 214
- Algorithmische Macht 125, 126
- Algorithmus 25, 43, 125, 126, 142
- Alles ist Zahl 65
- Allgemeine Datenschutzverordnung 75,
90, 109, 126, 297, 321
- Altruismus 2, 10, 13, 21, 26, 27, 29–38, 59,
143, 164, 168–172, 196, 198, 368
- Altruistisch 30, 32, 170
- Arbeitswerttheorie 151, 152, 154
- Auskunftsrecht 187

- Besitzrecht 73, 110, 165, 166, 169,
170, 204

- Chefinformationsbeamten 308
- China Data Valley 325
- Code 122–125, 139
- Copyright 139
- Cyberbetrug 358
- Cyberdiebstahl 358
- Cyberhegemonie 265, 347, 355, 356
- Cyberhegemonismus 351, 358
- Cyberkriminalität 60, 351, 358
- Cyberliberalismus 264, 265, 347, 358
- Cybermilitarismus 351, 358
- Cyberraum 139, 263, 264, 274, 297, 363
- Cybersicherheit 221, 223, 319, 325, 327,
333, 349, 358, 362
- Cybersouveränität 212
- Cyberterrorismus 351, 358, 362

- Datenanbieter 188
- Datenangriff 242, 243

- Datenanschauung 50
- Datenbetreiber 97
- Datenbetriebsrecht 97
- Datendienstleister 254
- Dateneigentumsrecht 28, 49, 56, 94, 98,
191, 205, 347, 360, 368
- Dateneigentumsrechtssystem 111, 134
- Datengleichheitsrecht 238, 239
- Datenhegemonie 229, 234, 255, 258, 268,
269, 270
- Datenhegemonismus 211, 257–259,
268, 271
- Datenidentität 86
- Dateninfrastruktur 234, 247, 250
- Datenkapital 201, 260
- Datenkapitalismus 211, 257, 258, 260,
261, 268
- Datenkontrolleur 86
- Datenlokalisierung 259, 269
- Datenlücke 116, 260
- Datenmacht 40, 63, 64, 81–86, 105, 106,
109, 110–115, 138
- Datenmissbrauch 99
- Datenmonopol 169, 211, 260
- Datennutzer 57, 233
- Datennutzung 28, 50, 52, 53, 57, 58, 64,
96, 99, 104, 106, 112, 125, 133, 162,
163, 168, 175, 177, 188, 191, 308,
319, 360, 368
- Datennutzungsrecht 191
- Datenöffnung 104, 341, 342
- Datenperson 1, 21–23, 25, 27–29, 32, 33,
38–40, 42, 44–46
- Datenperson-Hypothese 1, 21, 25, 27
- Datenpersönlichkeitsrecht 360
- Datenprotektionismus 211, 257–259, 268

- Datenraum 211, 212, 226, 229, 230, 232–235, 238, 239, 245, 247, 248, 250–254, 256–261
- Datenrecht 14, 28, 50, 59, 63, 64, 72, 81, 86, 93, 136, 140, 164, 166, 167, 168, 192, 194, 277, 279, 314, 327, 348, 359, 368, 371
- Datenrechte und -interessen 76, 86, 89, 106, 133, 136
- Datenrechtsgesetz 1, 21, 28, 29, 37–39, 53, 60, 177, 208, 209, 277, 327, 346–350, 359–363, 367, 368, 370, 371, 372
- Datenrechtsinhaber 192, 280, 297, 312, 323
- Datenrechtsschutz 121, 135, 173, 361
- Datenrechtssubjekt 86
- Datenrechtssystem 27, 38, 47, 48, 50–54, 57, 58, 60, 103, 117, 139, 208, 277, 279, 312, 327, 346, 348, 359, 368
- Datensammlung 175
- Datensatz 345
- Datenschicht 202
- Datenschutz 28, 52, 63, 75, 107, 125, 127, 131, 133–134, 136, 142, 166, 174, 177, 272, 281, 282, 284, 286, 293, 294, 296, 301, 302, 321, 360, 368
- Datensicherheit 28, 35, 38, 50, 95, 115, 118, 121, 128, 131, 162, 186, 211, 212, 221, 226, 234, 243, 245–248, 252–256, 260, 268, 271–273, 275, 295–299, 318–323, 325–329, 332, 361, 362, 365, 366
- Datensouveränität 52, 63, 71, 140, 211, 212, 219, 220, 223–225, 228, 229, 238, 240, 244, 245, 247, 248, 252, 253, 256–262, 267, 268, 271, 273–275, 319, 365
- Datensubjekt 96, 102
- Datenterrorismus 211, 255–258, 261, 268
- Datentransaktion 178, 189
- Datenunabhängigkeitsrecht 234–236
- Datenverwaltung 38, 82, 105, 119, 234, 240, 268
- Datenwert 27, 57, 143, 144, 164, 182, 183, 203, 206, 207
- Datenzirkulation 96, 173, 320
- Datenzuständigkeit 229–232, 238, 248, 250, 256
- Dezentralisierung 348
- Digitale Regierung 303, 310, 333, 334
- Digitale Wirtschaft 204, 372
- Digitale Zivilisation 28, 39, 164, 363, 368, 371
- Digitales China 334
- Digitalisierung 23, 55, 68, 116, 308
- Egoismus 13, 26, 31, 32, 34–36, 164, 169, 170, 197, 198, 259
- Egoistisch 18, 26, 29, 32, 33
- Eigentumsrecht 55, 56, 57, 60, 69, 73, 77, 91, 93, 94, 96–98, 102, 103, 104, 116, 122, 123, 136, 156, 163, 165, 190, 204, 205, 251
- Ein Recht für ein Ding 110, 166, 167
- Elektronische Persönlichkeit 43
- Ertragsrecht 178, 185, 189, 193, 194, 204, 205
- Ethiker 29
- Exklusivität 32, 70, 162, 165, 204
- Freiheitsrecht 157–160
- Fremddatenrecht 57
- Gerechtigkeit 5, 11, 12, 16, 18, 36, 48, 50, 57, 58, 74, 131, 139, 168, 169, 196, 199–201, 203, 207–209, 347, 350, 356, 357
- Globale Internet-Verwaltung 361
- Globales Gemeingebiet 262
- Grenzlosigkeit 223, 358
- Grenzüberschreitende Übertragung 72
- Grenzwerttheorie 151, 152

- Hobbes Dschungel 34
 Hypothese des Sozialmenschen 12, 13
 Hypothese des Wirtschaftsmenschen 11–14, 26
 Identifizierbarkeit 88
 Informationsrecht 138, 141
 Intelligente Regierung 309
 Intelligenter Roboter 41
- Knappheit 143, 148, 149, 152, 167, 169, 187, 191, 207
 Konfrontation 63, 105, 106, 245, 247, 248, 254
 Kontrollrecht 49, 89, 97, 99, 110, 165, 166, 190, 196, 355
 kulturelle Einbettbarkeit 13
- Leistungsverwaltung 157–159
- Machtstruktur 85, 86, 138, 139
 Mehrwert 104, 149, 150, 153, 181, 206, 341
 Mehrwerttheorie 153
 Menschenrecht 59, 293
 Mensch-Maschine-synergie 42
 Moderation der Legalisierung von Datenrechten 53
 Moderne Souveränität 218, 219
 Moralität 9, 62
 Multilaterale Verwaltung 265, 266
- Natürliche Person 44, 87, 88, 183, 279, 315
 Nießbrauchsdatenrecht 193, 194
 Notwendigkeitsprinzip 244
 Nutzungsrecht 49, 55–57, 60, 73, 77, 102, 103, 156, 163, 165, 166, 178, 185, 187, 188, 193–196, 204, 205
 Nutzungsrecht auf Gemeinnutzdaten 196
- Offene Daten 101, 343
 Offene Regierung 306
- Öffentliche Daten 49, 50, 144, 178–180, 183, 188, 194–196, 207, 342, 368
 Öffentliche Interessen 57, 82, 174, 176, 191, 195, 196, 199, 326
 Öffentliche Macht 81, 82, 84, 111–113, 115–118, 120
 Öffentliches Recht 115
 Öffnung der Regierungsdaten 104, 138, 345
 Öko-Mensch 23
- Persönliche Daten 74, 77, 81, 101, 114, 118, 144, 183, 279
 Persönliche Datenhoheit 224
 Persönliche Unterlagen 87
 Persönliches Datenrecht 86
 Persönlichkeitsrecht 69, 72, 89, 92, 93, 136, 209
 Position im Cyberspace 86
 PRISM-Vorfall 77
 Privatsphäre 22, 24, 69, 75, 77, 78, 81, 89, 90, 92, 95, 107, 108, 114, 115, 118, 119, 123, 126–128, 131, 137, 141, 142, 164, 173–177, 179, 180, 183, 209, 259, 264, 277, 279, 281–290, 293, 294, 297–299, 305, 313, 315, 327–329, 351, 365, 372
- Recht auf Gleichheit 157, 229, 230, 237, 238, 347
 Recht auf Privatsphäre 89, 90, 119, 127, 141, 164, 173–177, 285, 286, 289, 293, 297, 315, 372
 Recht auf Streben nach Glück 293
 Recht auf Teilhabe an öffentlichen Daten 179
 Recht auf Vergessen 50, 51, 89, 135, 173, 360
 Recht auf Vergessen von Daten 50, 51, 135, 360
 Rechtsbündel 72, 73, 99, 181

- Rechtssystem 27, 37, 40, 47, 48, 50, 63,
74, 99, 103, 106, III, 125, 128, 134,
136, 141, 162, 163, 241, 284, 286,
289, 292, 293, 297, 299, 312, 316,
361, 363, 365
- Regierungsdaten 51, 100–105, 133, 135,
138, 142, 305, 306, 310, 311, 330–
332, 336, 338, 339, 343–345
- Regierungsdatenrecht 86
- Regierungsverwaltung 68, 100, 277,
278, 303, 304, 306, 312, 333, 336,
337, 368
- Relativität 212, 226, 227, 231
- Roboter 22, 41, 41–44, 62, 279
- Rundes Gefängnis 176
- Sachenrecht 57
- Schicksalsgemeinschaft der Mensch-
heit 220, 277, 363
- Schlüsselinformationsinfrastruktur 319,
328, 352
- Schutz der Privatsphäre 24, 75, 95, 115,
126, 128, 176, 209, 259, 279, 281,
283, 286, 288–290, 298, 305
- Selbstverteidigungsrecht 229, 230, 241–
244
- Sensible Daten 80, 247, 328, 342
- Sophia 44
- Souveränitätsübertragung 249, 250
- Sozialität 8, 15, 26, 36, 38
- Staatliche Sicherheit 52, 179, 220, 227,
258, 266, 318
- Staatsouveränität 71, 213, 217, 220, 275
- Symbiont 42
- System der Legalisierung von Datenrech-
ten 48, 368
- Teilhaberecht 50, 73, 143, 157–161, 163–
170, 172–185, 197, 199–207, 348,
360, 368, 370, 372
- Teilhabewert 149, 153–157, 163, 164, 170,
190, 206
- Teilhabe-Wirtschaft 208
- Theorie der relativen Souveränität 228
- Theorie über Rechtsbündel 73
- Unabhängigkeitsrecht 233–235
- Unilateralismus 247, 260, 347, 348
- Unternehmensdaten 51, 95–99, 101, 133,
135, 137, 139, 140
- Unternehmensdatenrecht 86
- Verfügungsrecht 55, 56, 70, 97, 127,
165–167, 178, 185, 190, 191, 195,
196, 204
- Verfügungsrecht auf Gemeinnutz-
daten 196
- Verkauf von Cyberpyramiden 358
- Verwaltungsrecht 73, 103, 116, 195, 196,
312, 313, 360
- Verwaltungsrecht auf Gemeinnutz-
daten 195, 196
- Virtuelle Persönlichkeit 42
- Werttheorie 150–152, 154, 208
- Wiedervermischung 350, 370
- Zugriffsrecht 178, 185–187, 193