AUFSÄTZE

Datenschutz im Cloud-Computing nach chinesischem Recht

Jasper Habicht[1]

1. Einleitung

Im Zuge der Globalisierung und technischen Entwicklung ist das als „Cloud-Computing" bezeichnete Auslagern von elektronischer Datenverarbeitung weltweit zu einem immer stärker diskutierten Thema geworden. Auch in der Volksrepublik (VR) China[2] wird dem Cloud-Computing ein großes wirtschaftliches Potenzial beigemessen: Im aktuellen Fünfjahresplan für die Jahre 2011 bis 2015 hat sich die Regierung der VR China das Ziel gesetzt, die Internet-Industrie und insbesondere die Cloud-Computing-Branche zu fördern und auszubauen.[3] Nicht nur Privatkunden, sondern auch Organisationen und Konzerne nutzen vermehrt die Technik des Cloud-Computings, um aufwändige Rechenprozesse kostengünstig auszulagern. Das Outsourcen von Daten hat jedoch nicht nur Vorteile in Form von vermindertem Bedarf an vom Nutzer selbst bereitzustellender Hard- und Software und damit von Kostenersparnissen, sondern es birgt auch Risiken insbesondere für den Datenschutz. In China befindet sich der rechtliche Schutz von personenbezogenen Daten noch in seiner Ausgestaltungsphase, gleichwohl ist die rasche Weiterentwicklung auf diesem Gebiet ebenfalls ein erklärtes Ziel der Regierung: Im nationalen Strategiepapier für die Entwicklung der Informationalisierung für die Jahre 2006 bis 2020 wird der Ausbau des gesetzlichen Schutzes unter anderem von personenbezogenen Daten als ein zu erreichendes Ziel definiert.[4] Vor dem Hintergrund der internationalen Weiterentwicklung der Cloud-Computing-Branche und der damit einhergehenden Zunahme von Datenübertragungen zwischen Unternehmen und Einzelpersonen wird die Ausarbeitung eines rechtlich fundierten Datenschutzes in China zu einem immer relevanteren Thema.

Obgleich die etwas ältere Forschung häufig nur ein eher gering ausgeprägtes Bewusstsein für Privatsphäre in der chinesischen Bevölkerung nachzuweisen vermag,[5] können einzelne aktuelle Studien immerhin einen signifikanten Zusammenhang zwischen einem hohen Schutz von Privatsphäre und personenbezogenen Daten und einer Verringerung des wahrgenommenen Risikos beim Online-Kauf von Produkten durch chinesische Konsumenten zeigen.[6] So konnten LIU/FAN/JIANG (2009) in einer Studie nachweisen, dass von den Befragten besonders die Nummer der Bankkarte und des Ausweises sowie u.a. Angaben zur finanziellen Situation, Anschrift und Telefonnummer als schützenswert angesehen wurden.[7] Es ist also festzuhalten, dass auch in der chinesischen Bevölkerung offenbar ein erstarkendes Bewusstsein für den Datenschutz und dessen Notwendigkeit zu finden ist.[8] Dieses sich verstärkende Bedürfnis nach einem besseren Schutz von personenbezogenen Daten insbesondere im Bereich des Internet findet immer stärker auch Ein-

---

1 Jasper Habicht, Dipl.-Reg.-Wiss., ist wissenschaftliche Hilfskraft am Ostasiatischen Seminar der Universität zu Köln. E-Mail: jasper.habicht@uni-koeln.de. Der Autor dankt Herrn Knut Benjamin Pißler für wertvolle Anmerkungen.

2 Da in diesem Beitrag die rechtliche Situation in der VR China behandelt wird, ist im Folgenden mit dem Begriff „China" stets die VR China gemeint.

3 Programm des 12. Fünfjahresplans der VR China zur wirtschaftlichen und gesellschaftlichen Entwicklung des Volkes: Abschnitt 10, Punkt 1 und Abschnitt 13, Punkt 1.

4 Vgl. *HONG Hailin* (洪海林), Studie zum zivilrechtlichen Schutz von persönlichen Daten (Dissertation an der Southwest University of Political Science & Law) (个人信息的民法保护研究), Chongqing 2007, S. 156.

5 So kommt ZHANG Guangxing in einer Studie aus den Jahren 1993–95 zu dem Ergebnis, dass lediglich 10,1 % der Befragten meinten, dass die Veröffentlichung von Dingen, die andere nicht wissen sollten, ihr Leben erheblich beeinflusst. Immerhin 35,4 % sprachen von einem gewissen Einfluss, 24 % von einem geringen und 12,5 % von gar keinem Einfluss; vgl. *ZHANG Guangxing* (张广兴), Personal Rights in Social Development (社会发展中的人身权利), in: *XIA Yong* (夏勇), Toward an Age of Rights—A Perspective of the Civil Rights Development in China (走向权利的时代——中国公民权利发展研究), 2., erweiterte Auflage. Beijing 1999, S. 387 f.

6 Vgl. beispielhaft *PAN Yu/ZHANG Xing/GAO Li* (潘煜/张星/高丽), Research on the Determinants of Purchasing Intention in Online Shopping—From the Perspective of Trust and Perceived Risk (网络零售中影响消费者购买意愿因素研究——基于信任与感知风险的分析), in: China Industrial Economics (中国工业经济), Vol. 7, Beijing 2010, S. 115–124.

7 *LIU Yezheng/FAN Ju/JIANG Yuanchun* (刘业政/凡菊/姜元春), Internet Users' Privacy Concerns (网络用户隐私关心问题研究), in: Commercial Research (商业研究), Vol. 2, Harbin 2009, S. 24.

8 Nicht zuletzt ist dieses Bewusstsein vermutlich durch diverse Vorkommnisse des letzten Jahrzehnts wie beispielsweise die *Renrou-Sousuo*-Fälle geprägt worden.

gang in Gesetzesnormen. Bereits in den 2005 veröffentlichten „Ansichten des Büros des Staatsrates zur Beschleunigung der Entwicklung des E-Commerce" wird die Ausgestaltung von Gesetzesnormen zum Schutz von Privatsphäre und Datenquellen gefordert.[9] In der jüngeren Zeit, insbesondere ab 2009, sind in diesem Sinne verschiedene Rechtsnormen erlassen worden, die den Schutz von Privatsphäre und personenbezogenen Daten zum Ziel haben. Die Gesetzgebung im Bereich des Datenschutzes ist bis heute einer ständigen Weiterentwicklung unterworfen.

Für die wirtschaftliche Praxis ist die aktuelle rechtliche Situation des Datenschutzes für den Bereich des Cloud-Computing von Bedeutung, da die Cloud-Computing-Branche zunehmend international tätig ist. Für die weitere Internationalisierung dieses Industriezweiges ist die Betrachtung und das Verständnis von unterschiedlichen nationalen Rechtskreisen und der Entwicklungen in besonderen Rechtsbereichen von grundlegender Bedeutung. Für die Rechtstheorie ist die derzeitige Herausbildung des in China noch sehr jungen rechtlichen Phänomens des Datenschutzes von besonderem Interesse, da verschiedene, teilweise grundsätzliche Fragestellungen beispielsweise zu Persönlichkeitsrechten oder der Kodifizierung des Zivilrechts in die Diskussion mit einfließen und die Herausbildung datenschutzrechtlicher Regeln somit stets im Gesamtzusammenhang der Entwicklung des chinesischen Rechts betrachtet werden muss.

Erster Teil: Das rechtliche Umfeld – Definition von „Cloud-Computing"

2. Der Begriff des „Cloud-Computing"

Gemeint ist mit dem Begriff der „Cloud" ein extern verlagertes Netzwerk aus Rechnern, Anwendungen und Prozessen, auf das ein Anwender bei der Inanspruchnahme eines so genannten „Cloud-(Computing-)Services", also einer Dienstleistung, die auf dem Cloud-Computing beruht, zugreift.[10] Prinzipiell handelt es sich beim Cloud-Computing um das Auslagern von Daten und Rechenprozessen auf andere, über ein Netzwerk verbundene Rechner. Die Ausformung eines Cloud-Services kann sich je nach konkretem Bedarf erheblich unterscheiden. Das Ziel des Cloud-Computings ist es, über solche Netzwerke Skaleneffekte nutzbar zu machen und so Ressourcen und Kosten einzusparen.[11] Durch die Nutzung von Hard- und Software durch mehrere Einzelpersonen können Kapazitäten flexibel zugewiesen und genutzt werden. Konkret ist es beispielsweise für ein Unternehmen, das Cloud-Dienstleistungen nutzt, nicht nötig, teure Lizenzen für einzelne Softwarepakete selbst zu erwerben, da es die online bereitgestellte Software gemeinsam mit den anderen Kunden des Cloud-Services nutzen kann. Zudem ist sichergestellt, dass die bereitgestellte Software stets auf dem neuesten Stand ist; kosten- und zeitintensive Updates entfallen also für das Unternehmen.

Als grundlegende Definition für das „Cloud-Computing" kann die Definition des US-amerikanischen National Institute of Standards and Technology (NIST)[12] dienen. Die dem Büro für die Standardisierungsverwaltung der VR China[13] untergliederte Nationale Kommission für Standardisierungstechnik in der Datensicherheit[14] hat 2012 einen Entwurf für einen unverbindlichen[15] nationalen Standard für die „Grundlegenden Sicherheitsanforderungen für Cloud-Computing-Dienstleistungsanbieter von Regierungsbehörden" veröffentlicht, dessen Definition von Cloud-Computing[16] exakt der o.g. Definition des NIST entspricht.[17] Der Definition des NIST zufolge ist Cloud-Computing eine Dienstleistung, die in erster Linie vom Nutzer selbst angefordert und verwaltet wird. Der Anbieter stellt lediglich über das Internet die nötigen Ressourcen gebündelt zur Verfügung, wobei ausreichende Netzwerk- und Serverkapazitäten vonnöten sind, um einen reibungslosen und schnellen Zugriff zu gewährleisten. Die Ressourcen stehen üblicherweise modular zur Verfügung, so dass der Nutzer sie nach Belieben selbst zusammenstellen kann; hierdurch entsteht eine hohe Flexibilität. Zudem kann der Nutzer die Ressourcen steuern und überwachen, wozu ihm entsprechende Kontrollmechanismen und Anpassungsfunktionen zur Verfügung

---

9 Chin.: 国务院办公厅关于加快电子商务发展的若干意见. Dort zu finden unter Punkt 3, Unterpunkt 7.

10 Vgl. *Thilo Weichert,* Cloud-Computing und Datenschutz, in: Datenschutz und Datensicherheit, Nr. 10, Wiesbaden 2010, S. 679.

11 Vgl. *Thilo Weichert* (Fn. 10), S. 679.

12 *National Institute of Standards and Technology (NIST)/Peter Mell/Timothy Grance,* The NIST Definition of Cloud-Computing (NIST Special Publication 800-145), Gaithersburg 2011, S. 2.

13 In der VR China ist laut „Standardisierungsgesetz der VR China" (中华人民共和国标准化法) vom 29. Dezember 1988 (StandardG) das Büro für die Standardisierungsverwaltung der VR China für den Erlass von nationalen Standards zuständig. Das Büro trägt auch die Bezeichnung „Nationale Kommission für Standardisierungsverwaltung"; chin.: 中华人民共和国国家标准化管理局 bzw. 国家标准化管理委员会. Das StandardG findet sich in deutsch in *Frank Münzel (Hrsg.), Knut B. Pißler,* Chinas Recht, 29.12.1988, 2 (Normierungsgesetz der VR China), Hamburg 2013.

14 Chin.: 全国信息安全标准化技术委员会.

15 Verbindliche nationale Standards (强制性国家标) erhalten die Kennung „GB", unverbindliche nationale Standards (推荐性国家标) die Kennung „GB/T" und nationale technische Dokumente mit Normcharakter (国家标准化指导性技术文件) tragen die Kennung „GB/Z".

16 Chin.: 云计算.

17 Vgl. *General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China (AQSIQ)/Standardization Administration of the People's Republic of China (SAC)* (中华人民共和国国家质量监督检验检疫总局/中国国家标准化管理委员会), Information Security Techniques—Basic Requirements of Security for Cloud-Computing Service Provider of Government Department (Draft) (信息安全技术——政府部门云计算服务提供商安全基本要求 (草案)), ohne Ortsangabe [Beijing] ohne Jahresangabe [2012], S. 4 (Punkt 3.1).

gestellt werden.[18] Diese Charakteristika finden sich auch in der o.g. chinesischen Definition wieder.[19]

Der Norm des NIST zufolge lassen sich Cloud-Computing-Dienste in drei Dienstleistungstypen und vier Betriebsmodelle unterteilen. Dabei handelt es sich zunächst bei den Dienstleistungstypen um verschiedene Arten der Kombination von Software- und Hardware-Ressourcen.[20] Üblicherweise werden diese verschiedenen Typen als Ebenen dargestellt, die aufeinander aufbauen, oder als unterschiedliche Grade der Spezialisierung.[21] Die Einteilung des NIST lässt jedoch grundsätzlich auch Zwischenstufen zu, sodass im Einzelfall eine eindeutige Zuordnung nicht notwendigerweise möglich ist. Zuunterst findet sich die reine Bereitstellung von Hardware (Server, Netzwerke, Speicher oder Rechenleistung), die als „Infrastructure as a Service (IaaS)" bezeichnet wird. Software wird in diesem Falle nur in dem Maße angeboten, wie für den Betrieb der Hardware nötig ist.[22] Darauf aufbauend folgt die Bereitstellung einer so genannten Plattform – „Platform as a Service (PaaS)" –, d.h. zum einen von Hardware und zum anderen, darauf aufbauend, eines Betriebssystems sowie bestimmter Programmier-Bibliotheken. Das Bereitstellen von Speicherplatz für Internetseiten, zu dem üblicherweise auch der Zugriff auf den Einsatz von serverseitigen Programmiersprachen oder Datenbanken gehört, lässt sich beispielsweise grundsätzlich zu dieser Form des Cloud-Computings zählen.[23] Als dritte Stufe schließlich lässt sich „Software as a Service (SaaS)" definieren. Hier wird, aufbauend auf den oben beschriebenen Stufen, dem Anwender internetbasierte Software zur Verfügung gestellt. Da diese Software auf der Hardware des Cloud-Dienstleisters läuft, geht ein Großteil der Speicher- und Rechenleistung auf den Anbieter über. Beispiele für Cloud-Dienste, die in erster Linie solche SaaS-Dienstleistungen anbieten, sind Dropbox, Google Drive, Microsoft Skydrive etc. Diese Dienste stellen über Anwendungen, die über einen üblichen Internetbrowser bedienbar sind, eine Schnittstelle zur Verwaltung und Bearbeitung von Daten bereit.[24] Obwohl eine solche Aufteilung nach unterschiedlichen Dienstleistungstypen des Cloud-Computings in der genannten chinesischen Norm nicht vorgenommen wird, findet sich jedoch in der chinesischen Literatur eine vergleichbare Unterteilung in „Infrastructure as a Service"[25], „Data Storage as a Service"[26], „Platform as a Service"[27] sowie „Software as a Service"[28].

Die vier verschiedenen Betriebsmodelle der NIST-Norm stellen verschiedene Stufen der Öffentlichkeit von Clouds dar, wobei auch hier eine Einordnung im Einzelfall nicht immer ganz trennscharf geschehen kann. Eine solche Unterteilung von Cloud-Diensten nach Betriebsmodell mit analogen Begriffen findet sich ebenfalls in der chinesischen Literatur.[29] Eine private Cloud („private cloud") ist dabei als ein Netzwerk zu verstehen, das gänzlich unter der Kontrolle einer einzigen Organisation steht, da es ausschließlich von dieser betrieben wird, und zu dem lediglich die Mitarbeiter dieser Organisation Zugang haben. Ein Zugriff von außen findet in diesem Falle nicht statt.[30] Dem gegenüber steht die öffentliche Cloud („public cloud"), die von einem Dienstleister angeboten und verwaltet wird und deren Nutzung jedermann offen steht.[31] Dies bedeutet allerdings nicht, dass jeder auf alle Inhalte der Cloud zugreifen kann. Vielmehr sorgt in einer öffentlichen Cloud eine umfassende Rechteverwaltung für den ordnungsgemäßen Zugriff auf Daten durch die verschiedenen Nutzer. Als Zwischenstufe zwischen privater und öffentlicher Cloud lässt sich die gemeinschaftliche Cloud („community cloud") identifizieren, die nur einem bestimmten Nutzerkreis offensteht.[32] Zuletzt führt das NIST die Konstruktion einer hybriden Cloud („hybrid cloud") an, womit Mischformen gemeint sind, beispielsweise wenn die Kapazitäten einer privaten Cloud nicht ausreichen und auf eine öffentliche Cloud als Ergänzung zurückgegriffen werden muss. Wichtig ist in dieser letzten Kategorie, dass die einzelnen Cloud-Formen für sich gesehen weiterbestehen, aber durch bestimmte Kanäle miteinander verbunden sind.[33]

Grundsätzlich lässt sich festhalten, dass private Clouds naturgemäß zwar sicherer, jedoch auch kostenintensiver für den Betreiber sind. Öffentliche

---

18 Vgl. *NIST/Peter Mell/Timothy Grance* (Fn. 12), S. 2.

19 Vgl. *AQSIQ/SAC* (Fn. 16), S. 4 (Punkt 3.1).

20 Die Unterteilung in drei Dienstleistungstypen ist dabei nicht erschöpfend. Andere Autoren führen weitere Dienstleistungsarten an, wie z.B. „(Data) Storage as a Service" oder „High Performance Computing as a Service"; vgl. bspw. *Thilo Weichert* (Fn. 10), S. 679, oder *CCID Consulting* (赛迪顾问股份有限公司), Weißbuch zur Entwicklung der Cloud-Computing-Branche in China (中国云计算产业发展白皮书), O.O. [Beijing] 2011, <http://www.ccidconsulting.com/ei/lib/down/20110509154002.pdf> eingesehen am 1. Juni 2013, S. 4.

21 So bspw. bei *Peter H. Deussen/Linda Strick/Johannes Peters,* Cloud-Computing für die öffentliche Verwaltung: ISPRAT-Studie November 2010, Berlin 2010, S. 16.

22 Vgl. *NIST/Peter Mell/Timothy Grance* (Fn. 12), S. 3; vgl. ähnlich *Peter H. Deussen/Linda Strick/Johannes Peters* (Fn. 20), S. 18.

23 Vgl. *NIST/Peter Mell/Timothy Grance* (Fn. 12), S. 2 f.; vgl. ähnlich *Peter H. Deussen/Linda Strick/Johannes Peters* (Fn. 20), S. 17.

24 *Vgl. NIST/Peter Mell/Timothy Grance* (Fn. 12), S. 2; vgl. *Peter H. Deussen/Linda Strick/Johannes Peters* (Fn. 20), S. 16 f.

25 Chin.: 基础架构即服务.

26 Chin.: 数据存储即服务.

27 Chin.: 平台即服务.

28 Chin.: 软件即服务; vgl. für alle Begriffe *CCIC Consulting* (Fn. 19), S. 3.

29 Vgl. *CCIC Consulting* (Fn. 19), S. 4; *WANG Jipei/LIU Shifeng* (王继培/刘世峰), Formulation of the Small-and-Medium-Sized Port Enterprise Cloud-Computing Model (中小港口企业云计算模型的构建), in: Logistics Technology (技术与方法), Vol. 30, No. 4, Xiangyang 2011, S. 83 f.

30 Vgl. *Peter H. Deussen/Linda Strick/Johannes Peters* (Fn. 20), S. 20 f.

31 Vgl. *Peter H. Deussen/Linda Strick/Johannes Peters* (Fn. 20), S. 22 f.

32 Vgl. *Peter H. Deussen/Linda Strick/Johannes Peters* (Fn. 20), S. 21 f.

33 Vgl. NIST/Peter Mell/Timothy Grance (Fn. 12), S. 3; vgl. auch Peter H. Deussen/Linda Strick/Johannes Peters (Fn. 20), S. 23.

Clouds, die von einer dritten Seite betreut werden, werden in der Regel nur nach der Nutzung bezahlt, was häufig zu Kostenersparnissen führt. Bei der Übertragung von Daten und deren Verarbeitung außerhalb des Unternehmens entstehen jedoch Sicherheitsrisiken, gegen die in technischer wie rechtlicher Hinsicht Schutzmaßnahmen zu ergreifen sind.[34] Hinsichtlich der Klassifizierung nach Dienstleistungstyp und Betriebsmodell kann zudem – zusammenfassend betrachtet – von einem international grundsätzlich einheitlichen Begriff des Cloud-Computings ausgegangen werden.

3. Cloud-Computing und der Transfer personenbezogener Daten in der rechtlichen Betrachtung

Im Folgenden soll Cloud-Computing als Nutzung von Hard- und Software Dritter über das Internet betrachtet werden. Der Nutzer überträgt dabei Daten an den Anbieter, die dann von diesem gespeichert oder verarbeitet werden. Die Speicherung und Verarbeitung wird zwar vom Nutzer veranlasst und zum großen Teil auch kontrolliert, die konkrete Ausführung liegt jedoch in der Macht des Anbieters, da nur dieser letztlich eine direkte Kontrolle über die zur Verfügung gestellten Dienste hat. Auf welchen konkreten Datenträgern beispielsweise die vom Nutzer übertragenen Daten gespeichert werden oder unter Zuhilfenahme welcher konkreter Algorithmen und Rechenprozesse die Daten verarbeitet werden, kann der Nutzer unter Umständen nicht beeinflussen.[35] Daher gewinnt die Nutzung von Cloud-Diensten insbesondere dann rechtliche Relevanz, wenn Nutzer und Anbieter verschiedenen rechtlichen Instanzen zugeordnet sind. Bei der Nutzung von privaten Clouds verbleiben die Daten üblicherweise bei der jeweiligen Organisation, weswegen eine entsprechende Kontrolle kein allzu großes Problem darstellt. Es soll daher im Folgenden der Schwerpunkt auf nicht-private Clouds gelegt werden, bei denen Nutzer und Anbieter verschiedenen Rechtssubjekten zugeordnet sind.

Es besteht in diesem Falle die Möglichkeit, dass der Anbieter einer SaaS-Dienstleistung beispielsweise seinerseits auf andere Dienstleister zurückgreift, die Hardware für seine Dienste bereitstellen. Genauso ist es möglich, dass der Nutzer eines Cloud-Dienstes die in der Cloud zu verarbeitenden Daten von einem Dritten erhalten hat, beispielsweise dann, wenn er selbst ein Unternehmen ist, das die Verwaltung von Kundendaten über einen Cloud-Anbieter abwickelt. Somit entsteht also eine unter Umständen sehr lange Kette von beteiligten Instanzen, die bestimmte Daten weiterreichen. Je mehr solcher Instanzen an der Datenverarbeitung beteiligt sind, desto schwieriger wird es naturgemäß für den Betroffenen bzw. für denjenigen, der die Daten zur Verarbeitung aufgibt, nachzuvollziehen, wo konkret was mit diesen Daten geschieht. Besonders problematisch ist dies bei sensiblen Daten, beispielsweise bei Daten, die auf die Identität von Individuen zurückschließen lassen.

Ein dem Cloud-Computing zugrunde liegendes rechtliches Problem ist der Schutz personenbezogener Daten, besonders dann, wenn diese an Dritte weitergegeben werden.[36] Insbesondere bei der Nutzung von Cloud-Diensten durch Unternehmen ist der Fall der Weitergabe von persönlichen Daten von Kunden an einen Cloud-Dienstleister eine rechtlich problematische Konstruktion, da in diesem Falle der Kunde des Unternehmens naturgemäß nur eine sehr geringe Kontrolle über die Verarbeitung der ihm zuordenbaren Daten hat. Ähnliches gilt entsprechend für persönliche Daten von Mitarbeitern eines Unternehmens. Eine rechtliche Konkretisierung ist an dieser Stelle besonders für das chinesische Recht erforderlich. Obgleich eine gewisse Grundlage für den Datenschutz bereits recht früh gleichsam mit der Schutzbedürftigkeit der Privatsphäre durch den Obersten Volksgerichtshof der VR China (OVG) bestätigt wurde,[37] hat der Schutz personenbezogener Daten im chinesischen Recht lediglich in diversen Einzelnormen, nicht aber in einem zusammenhängenden und umfassenden Gesetz Niederschlag gefunden.

Für den speziellen Fall des Auslagerns von Daten zur Verarbeitung durch eine andere Stelle kennt das deutsche Bundesdatenschutzgesetz (BDSG) das Konzept der „Auftragsdatenverarbeitung".[38] Sie greift, wenn personenbezogene Daten Dritter im Auftrag durch eine andere Stelle erhoben, verarbeitet oder genutzt werden, die Verantwort-

---

[34] Vgl. *Fabian Niemann/Jörg-Alexander Paul,* Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud-Computings, in: Kommunikation und Recht, Heft 7/8, Frankfurt a.M. 2009, S. 445; *WANG Jipei/LIU Shifeng* (Fn. 25), S. 83 f.

[35] Hansen verweist darauf, dass dem Nutzer bei der Bearbeitung seiner Daten unter Umständen gar nicht bewusst ist, dass diese im Moment seiner Bearbeitung in der Cloud verarbeitet werden, also bereits ein Datentransfer stattfindet. Zudem unterstreicht Hansen die Kontrollmacht des Cloud-Dienstleisters, wenn sie betont, dass bei SaaS-Angeboten mit Verschlüsselung der Anbieter oft über eine Entschlüsselungsmöglichkeit verfügt oder dies rechtlich sogar vorgesehen ist; vgl. *Marit Hansen,* Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter, in: Datenschutz und Datensicherheit, Nr. 6, Wiesbaden 2012, S. 407 und 410.

[36] Vgl. *Thilo Weichert* (Fn. 10), S. 681.

[37] Konkretisiert wurde das Recht auf Privatsphäre bereits in den „Ansichten (versuchsweise) des OVG zu einigen Fragen betreffend der Implementierung und Ausführung der „Allgemeinen Grundsätze des Zivilrechts der VR China"" (最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见 (试行)) vom 26. Januar 1988 (AGZAns), Gazette of the Supreme People's Court of the People's Republic of China (中华人民共和国最高人民法院公报), No. 2, Peking 1988, S. 19–36; vgl. hierzu Punkt 5.1.

[38] S. § 11 „Bundesdatenschutzgesetz [der Bundesrepublik Deutschland] i.d.F der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814)" (BDSG).

lichkeit für die Verarbeitung jedoch beim Auftraggeber verbleibt.[39] Da es sich bei den transferierten Daten nicht um Daten des Unternehmens selbst handelt, fordert das BDSG bei Transfer und Verarbeitung dieser Daten an bzw. durch Dritte besondere Schutzauflagen. Hervorzuheben sind hierbei die verschiedenen Rechte des Betroffenen (d.h. des Datensubjekts), die nicht durch ein Rechtsgeschäft begrenzt werden.[40] Grundsätzlich geht das BDSG bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten von einem Verarbeitungsverbot mit Erlaubnisvorbehalt aus, ohne eine Einwilligung des Betroffenen oder eine Erlaubnis durch ein Gesetz dürften folglich personenbezogene Daten in keiner Weise verarbeitet werden.[41] Die Auftragsdatenverarbeitung erfolgt nach BDSG regelmäßig über einen schriftlichen Vertrag, den der Auftragsgeber mit dem Auftragsnehmer schließt.[42] Die Verantwortung für den Schutz der Daten verbleibt dabei beim Auftragsgeber, dem gegenüber das Datensubjekt seine Rechte in Form von Schadensersatzansprüchen geltend machen kann.[43] Der Auftragsnehmer ist jedoch nicht vollständig seiner Schutzauflagen entbunden, so hat er für die technischen und organisatorischen Maßnahmen zum Schutz der Daten sowie für die Wahrung des Datengeheimnisses seinerseits zu sorgen.[44]

In China existiert bisher kein einheitliches Datenschutzgesetz, trotz Bestrebungen ein solches zu erlassen.[45] Das chinesische Recht kennt auch eine Verarbeitung von Daten im Auftrag nicht. Einige der bestehenden Normen definieren jedoch die zu schützenden Daten nicht in dem Sinne, dass sie sich ausschließlich dem Kunden eines Internetdienstanbieters (ISP) zuordnen lassen, so dass grundsätzlich nicht nur Daten aus einem Dienstleister-Kundenverhältnis von den Normen geschützt werden.[46] Des Weiteren beziehen sich einzelne Normen allgemein auf die Weitergabe von Daten an Dritte, so verbietet das chinesische Strafgesetzbuch von 2009 (StGB) die illegale Weitergabe von persönlichen Daten an Dritte.[47]

Zweiter Teil: Die rechtlichen Schutzgüter

4. Aspekte von Privatsphäre und Datenschutz im chinesischen Recht

Bevor auf die einzelnen rechtlichen Regelungen mit Bezug zu Privatsphäre und Datenschutz im Internet und insbesondere zu datenschutzrechtlichen Aspekten des Cloud-Computings eingegangen wird, soll zunächst geklärt werden, was grundsätzlich in der chinesischen Rechtslehre unter „Privatsphäre" zu verstehen ist, wie sich der Schutz der Privatsphäre im Recht manifestiert und auf welche Weise sich das Recht auf Privatsphäre aus höherem Recht ableitet. Zudem soll gleichzeitig beleuchtet werden, ob und inwiefern sich aus dem Recht auf Privatsphäre ein Schutz von personenbezogenen Daten ableiten lässt und wie dessen rechtlichen Aspekte im chinesischen Recht umgesetzt sind. Der Fokus soll stets auf dem Schutz personenbezogener Daten liegen. Bei der Betrachtung soll punktuell auf das deutsche Recht vergleichend eingegangen werden.

Daran anknüpfend soll die Entwicklung datenschutzrechtlicher Normen vor dem Hintergrund der veränderten gesellschaftlichen Bedürfnisse im Zuge der Ausbildung einer Informationsgesellschaft in China betrachtet werden.

4.1 Rechtliche Ausgestaltung von Privatsphäre und Datenschutz

Da der Schutz personenbezogener Daten international ein relativ neues Problem ist, das insbesondere durch die rasche Entwicklung der EDV entstanden ist, die eine Verarbeitung und Übermittlung großer Mengen von Daten in kurzer Zeit ermöglicht, ist in vielen Rechtsordnungen ein solcher Schutz erst in neuerer Zeit aus bereits bestehenden

---

[39] Das BDSG kennt ferner die „Funktionsübertragung", bei der auch die Verantwortung für die Verarbeitung auf den Auftragnehmer übergeht. Bei der Nutzung von Cloud-Diensten ist jedoch regelmäßig das rechtliche Konstrukt der Auftragsdatenverarbeitung maßgeblich; vgl. *Thilo Weichert* (Fn. 10), S. 683.

[40] Vgl. §§ 33 Abs. 1, 34 Abs. 1, 35 Abs. 1–4 BDSG; *Sven Polenz,* Teil 13: Datenschutz, in: *Wolfgang Kilian/Benno Heussen* (Hrsg.), Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis. Loseblattsammlung, 31. Ergänzungslieferung, München 2012, Betroffenenrechte: Rn. 1.

[41] Vgl. § 4 Abs. 1 BDSG; *Marian Alexander Arning/Nils Christian Haag,* Kapitel II. Datenschutz, in: *Joerg Heidrich/Nikolaus Forgó/Thorsten Feldmann* (Hrsg.), Heise Online-Recht: Der Leitfaden für Praktiker & Juristen, Loseblattsammlung, 3. Ergänzungslieferung, Hannover 2011, Rn. 17; *Sven Polenz* (Fn. 36), Verfassungsrechtliche Grundlagen des Datenschutzes: Rn. 4.

[42] Vgl. *Sven Polenz* (Fn. 36), Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes: Rn. 50.

[43] Vgl. § 11 Abs. 1 BDSG; *Sven Polenz* (Fn. 36), Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes: Rn. 54.

[44] Vgl. *Sven Polenz* (Fn. 36), Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes: Rn. 56.

[45] S. hierzu ausführlich Punkt 11.1 und 11.2.

[46] So spricht bspw. § 253-1 „Strafgesetzbuch der VR China" (中华人民共和国刑法) vom 28. Februar 2009 (StGB) allgemein von „persönlichen Daten von Bürgern", ähnlich sanktioniert § 36 „Deliktshaftungsgesetz der VR China" (中华人民共和国侵权责任法) vom 26. Dezember 2009 (DelHaftG) allgemein die „Verletzung von Rechten Dritter" durch Internetnutzer oder ISP. S. zur Begriffsdefinition ausführlich Punkt 9.2.

Das StGB von 1997 findet sich in Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 10, Peking 1997, S. 419–495; die hier relevanten Änderungen der siebten Revision finden sich in Gazette of the Standing Committee of the National People's Congress of the People's Republic of China (中华人民共和国全国人民代表大会常务委员会公报), No. 2, Peking 2009, S. 187–189; das DelHaftG findet sich in Gazette of the Standing Committee of the National People's Congress of the People's Republic of China (中华人民共和国全国人民代表大会常务委员会公报), No. 1, Peking 2010, S. 4–10.

[47] Vgl. § 253-1 StGB; s. ausführlich Punkt 6.1.

Rechtsnormen abgeleitet oder ausgearbeitet worden. Auch in China ist ein Schutz der Privatsphäre sowie der persönlichen Daten erst in jüngerer Zeit rechtlich kodifiziert worden.

In China fehlt es an einem Gericht, das die Verfassung interpretieren kann. Eine Einklagbarkeit der Grundrechte ist für den Bürger daher grundsätzlich nicht gegeben.[48] Im Gegensatz zum deutschen Konstrukt des allgemeinen Persönlichkeitsrechts, das aus Art. 1 Abs. 1 (Unantastbarkeit der Würde des Menschen) i.V.m. Art. 2 Abs. 1 Grundgesetz (Recht auf freie Entfaltung der Persönlichkeit) durch richterliche Rechtsfortbildung abgeleitet wird,[49] und seinen Derivaten, insbesondere dam Recht auf informationelle Selbstbestimmung, die als Grundrechte über die mittelbaren Drittwirkung auch in das Privatrecht ausstrahlen,[50] kann die Frage, ob Grundrechte aus der chinesischen Verfassung ebenfalls in privatrechtliche Beziehungen hineinstrahlen können, im Allgemeinen nicht bejaht werden.[51]

Gleichwohl ist die chinesische Verfassung als höchste Rechtsnorm anerkannt, deren Regeln sich alle untergeordneten Normen beugen müssen.[52] Die chinesische Verfassung von 1982 definiert in ihrem zweiten Kapitel Grundrechte und Grundpflichten der Bürger. Insbesondere sind hier die Artikel 37, 38, 39 und 40 zu nennen, die die Privatsphäre von Bürgern betreffen. Artikel 37 definiert zunächst das Habeas-Corpus-Prinzip, nach dem die Freiheit der Bürger unverletzlich ist und eine Verhaftung nur vorbehaltlich einer Entscheidung der Volksstaatsanwaltschaft oder einer richterlichen Entscheidung erfolgen darf.[53] Artikel 38 statuiert die Unverletzlichkeit der Würde der Person und verbietet jegliche Form von Beleidigung, Verleumdung und Diffamierung.[54] Artikel 39 definiert die Wohnung als unverletzlich[55] und Artikel 40 garantiert die Freiheit und das Geheimnis der Korrespondenz.[56] Artikel 40 schränkt jedoch die Freiheit und das Geheimnis der Korrespondenz insoweit ein, als für die Bedürfnisse der staatlichen Sicherheit oder zwecks Aufklärung von Straftaten Organe der öffentlichen Sicherheit oder der Staatsanwaltschaft auf gesetzlicher Grundlage eine Zensur vornehmen können.[57] In der Literatur wird zum Teil die in der Verfassung festgeschriebene Unverletzlichkeit der Wohnung und des Brief- und Kommunikationsgeheimnisses als Grundlage für ein Recht auf Privatsphäre interpretiert, wie es seit 2009 im Delikthaftungsgesetz (DelHaftG) zu finden ist.[58]

Obgleich das Recht auf Privatsphäre seit 2009 zumindest im Privatrecht kodifiziert ist, fehlt eine einheitliche Definition. In der juristischen Diskussion über die rechtliche Qualität von Privatsphäre wird in der Literatur oft auf den US-amerikanischen Begriff des „Right to Privacy" rekurriert oder auf ein allgemeines Persönlichkeitsrecht nach deutschem Muster Bezug genommen.[59] Im Fokus der Betrachtung soll an dieser Stelle die Frage stehen, inwiefern das Recht auf Privatsphäre auf den Schutz personenbezogener Daten anwendbar ist. Eine juristische Definition des Rechts auf Privatsphäre im Sinne des DelHaftG liefert WANG Shengming, wonach das Recht auf Privatsphäre „das Persönlichkeitsrecht einer natürlichen Person, über ihre persönlichen, nicht das Interesse der Öffentlichkeit oder der Allgemeinheit berührenden personenbezogenen Daten, privaten Aktivitäten und privaten Bereiche verfügen zu können" meint.[60] WANG Liming (2005) sieht das Recht auf Privatsphäre ebenfalls auf natürliche Personen beschränkt,

---

48 Vgl. *Simon Werthwein,* Das Persönlichkeitsrecht im Privatrecht der VR China, Berlin 2009, S. 20.

49 Vgl. BVerfGE 65, 1 ff.; vgl. *Udo Di Fabio,* GG Art. 2, in: *Theodor Maunz/Günter Dürig,* Grundgesetz-Kommentar, Loseblattsammlung, 67. Ergänzungslieferung, München 2013, Rn. 128; *Heinrich Lang,* BeckOK GG Art. 2, in: *Volker Epping/Christian Hillgruber (Hrsg.),* Beck'scher Online-Kommentar GG, Edition 17, München 2013, Rn. 32 f.; *Spiros Simitis,* Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, in: Neue Juristische Wochenschrift 1984, München 1984, S. 399.

50 Vgl. *Heinrich Lang* (Fn. 45), Rn. 45; *Udo Di Fabio* (Fn. 45), Rn. 191; *Sven Polenz* (Fn. 36), Verfassungsrechtliche Grundlagen des Datenschutzes: Rn. 8; *Spiros Simitis* (Fn. 45), S. 401.

51 Die Problematik ist besonders durch den *QI-Yuling*-Fall in die Diskussion geraten. Der OVG hatte im Jahr 2008 seine ursprüngliche Interpretation, dass in gewissen Fällen verfassungsmäßig garantierte Grundrechte auch im Zivilrecht zur Anwendung kommen können, wieder zurückgezogen; vgl. *Thomas E. Kellogg,* The Death of Constitutional Litigation in China?, in: ChinaBrief, Vol. 9, No. 7, Washington 2009, S. 4.

52 So verlangt es u.a. auch § 3 des „Gesetzgebungsgesetzes der VR China" (中华人民共和国立法法) vom 15. März 2000, zu finden in Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 13, Peking 2000, S. 7–16.

53 Vgl. Art. 37 „Verfassung der VR China" (中华人民共和国宪法) vom 4. Dezember 1982 (Verf), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 20, Peking 1982, S. 851–874; deutsche Übersetzung in *Robert Heuser,* „Sozialistischer Rechtsstaat" und Verwaltungsrecht in der VR China (1982–2002), Hamburg 2003, S. 207–243.

54 Vgl. Art. 38 Verf.

55 Vgl. Art. 39 Verf.

56 Vgl. auch *MA Yichan* (马屹婵), Prevention and Relief of Online Speech Invasion of Privacy Laws (网络言论侵犯隐私权的法律防范与救济), in: Journal of Changchun Institute of Technology (Social Science Edition) (长春工程学院学报 (社会科学版)), Vol. 13, No. 3, Changchun 2012, S. 39.

57 Vgl. Art. 40 Verf.

58 Vgl. *WANG Liming* (王利明), Re-definition of Right to Privacy (隐私权概念的再界定), in: The Jurist (法学家), Vol. 1, Beijing 2012, S. 110.

59 Vgl. bspw. *SHEN Che/XU Wenjie* (沈中/许文洁), On the Right to Privacy and Personality (隐私权论兼析人格权), Shanghai 2010, S. 90 f.; *QI Aimin* (齐爱民), Grundsätze eines Personendatenschutzgesetzes und rechtliche Fragen zum internationalen Datenaustausch (个人资料保护法原理及其跨国流通法律问题研究), Wuhan 2004, S. 22 f.; *WANG Liming* (王利明), On Personality Rights Law (人格权法研究), Beijing 2005, S. 559 f.; SHEN/XU bieten zudem eine umfassende Diskussion zu dem Begriff „Privatsphäre" (隐私) und der Definition des „Rechts auf Privatsphäre" (隐私权). SUN merkt zudem an, dass die Übersetzung des englischen Begriffs „privacy" mit dem chinesischen Wort 隐私 neueren Ursprungs ist und in chinesischen Übersetzungen von internationalen Verträgen wie der UN-Menschenrechtserklärung oder dem UN-Zivilpakt „Privatsphäre" mit dem Begriff „私生活" übersetzt wird; vgl. *SUN Jianjiang* (孙建江), A Criticism of the Conception of "Yin Si" ("隐私" 的概念质疑), in: Journal of Graduate School of Chinese Academy of Social Sciences (中国社会科学院研究生院学报), No. 2, Beijing 2010, S. 80 f.

60 *WANG Shengming* (王胜明), Erläuterungen zum Delikthaftungsgesetz der VR China (中华人民共和国侵权责任法释义), Beijing 2010, S. 24.

jedoch nicht nur auf Bürger.[61] Den Gegenstand des Rechts fasst WANG Liming äußerst weit, so dass auch ein grundsätzlicher Schutz personenbezogener Daten ableitbar ist. Privatsphäre unterteilt sich nach WANG in das „private Informationsgeheimnis"[62] und den „Frieden des Privatlebens"[63], wobei das Informationsgeheimnis alle Informationen umfasst, die eine Privatperson nicht der Öffentlichkeit preisgeben will, solange diese Informationen nicht rechtswidrig sind oder die „gesellschaftlich-öffentliche Moral"[64] verletzen.[65]

Wenngleich in einem Großteil der älteren Literatur „persönliche Daten"[66] als ein Bestandteil von Privatsphäre definiert werden,[67] ist in der neueren chinesischen Literatur vermehrt die Ansicht vertreten, dass der Schutz personenbezogener Daten nicht unter das Recht auf Privatsphäre subsumiert werden kann. So sehen beispielsweise HU/ZHENG nicht die Gesamtheit der personenbezogenen Daten vom Recht auf Privatsphäre, wie es in der aktuellen chinesischen Rechtsprechung in Erscheinung tritt, geschützt, sondern insbesondere lediglich diejenigen personenbezogenen Daten, die für die Allgemeinheit nicht von Interesse sind.[68] Abgesehen von der unterschiedlichen Qualität der bei Rechtsverletzung entstehenden Schäden[69] sehen HU/ZHENG einen fundamentalen Unterschied zwischen Privatsphäre und personenbezogenen Daten darin, dass erstere nicht an Dritte weitergegeben werden kann, letztere – zumindest was ihren materiellen Wert betrifft – jedoch sehr wohl.[70] Aus diesem Grund fordern HU/ZHENG die Einführung eines weiteren konkreten Persönlichkeitsrechts, das den Schutz von personenbezogenen Daten zum Gegenstand hat.[71] Auch ZHANG Zhenliang kommt zu dem Schluss, dass das „Recht an den persönlichen Daten"[72] weder als Eigentumsrecht auftritt, noch dem Recht auf Privatsphäre zugeordnet werden kann, sondern ein eigenständiges Persönlichkeitsrecht ist,[73] das insbesondere ein Recht auf informationelle Selbstbestimmung, ein Recht auf Geheimhaltung, Berichtigung, Sperrung, Löschung, Auskunft über die Verarbeitung und Vergütung der Nutzung der eigenen personenbezogenen Daten, sowie Rechtsansprüche wie Unterlassung oder Entschädigung umfasst.[74] Fragwürdig bei der Subsumierung des Rechts an den persönlichen Daten unter das Recht auf Privatsphäre ist jedenfalls die Schutzwürdigkeit von bereits (freiwillig) veröffentlichten Daten.[75]

WANG Liming sieht in seinen neueren Publikationen für einen umfassenden Persönlichkeitsrechtsschutz im chinesischen Rechtssystem die Begründung eines „allgemeinen Persönlichkeitsrechts" als notwendig an, da das Recht auf Privatsphäre nicht die Qualität und dem Umfang eines solchen allgemeinen Persönlichkeitsrechts hat. Das Recht auf Privatsphäre sei, gleichsam den übrigen Persönlichkeitsrechten (wie sie z.B. in § 2 Abs. 2 DelHaftG definiert werden), diesem allgemeinen Persönlichkeitsrecht unterzuordnen, das allgemein gefasst den Schutz der Menschenwürde sowie der persönlichen Freiheit zum Inhalt habe.[76] Das Recht auf Privatsphäre und das Recht auf den Schutz von personenbezogenen Daten sieht WANG damit als zwei voneinander getrennte Rechte an, die sich sowohl hinsichtlich ihrer Zielsetzung als auch in ihrer rechtlichen Qualität unterscheiden.[77] Während das Recht auf Privatsphäre den Schutz des Individuums vor unerwünschtem Eindringen in seinen privaten Lebensbereich zum Ziel habe und daher als Abwehrrecht ausgestaltet sei, aus welchem dem Einzelnen entsprechende Rechtsansprüche erwach-

---

61 Vgl. *WANG Liming* (2005) (Fn. 55), S. 590 f.; WANG bezieht sich hier auf das Recht auf Privatsphäre im Sinne der AGZAns bzw. RufReAntw.

62 Chin.: 私人信息秘密.

63 Chin.: 私生活安宁.

64 Chin.: 社会公共道德.

65 *WANG Liming* (2005) (Fn. 55), S. 594 ff.

66 Chin.: 个人信息. Korrekterweise ist der chinesische Ausdruck mit „persönliche Informationen" zu übersetzen. Teilweise werden in der chinesischen Literatur die Formulierungen „persönliche Informationen" (个人信息) und „persönliche Daten" (个人数据) nebeneinander verwendet. Da jedoch kein bedeutungsrelevanter Unterschied zwischen beiden Begriffen zu erkennen ist, werden im Folgenden beide Begriffe mit der im Deutschen üblichen Formulierung „persönliche Daten" übersetzt. In diesem Beitrag wird allerdings grundsätzlich der Begriff „personenbezogene Daten" verwendet, der Begriff „persönliche Daten" bezieht sich als wörtliche Übersetzung stets auf eine bestimmte rechtliche Definition.

67 So wird Privatsphäre beispielsweise in „persönliche Daten", „persönliche Aktivitäten" und den „persönlichen Bereich" oder in „persönliche Daten", das „persönliche Lebensumfeld" und „persönliche Angelegenheiten" unterteilt; vgl. *WANG Shengming* (Fn. 56), S. 24; *ZHANG Zhenliang* (张振亮), Right of Personal Information and Its Civil Law Protection (个人信息权及其民法保护), in: Journal of Nanjing University of Posts and Telecommunications (Social Science) (南京邮电大学学报 (社会科学版)), Vol. 9, No. 1, Nanjing 2007, S. 41; *WANG Liming* (王利明) et al., A Propositional Version with Legislative Reasons for Civil Code Draft of China—Publicity Rights, Marriage and Family, Inheritance (中国民法典学者建议稿及立法理由——人格权编、婚姻家庭编、继承编), Beijing 2005, S. 147; *WU Yanfen/MA Qinghong* (武艳芬/马青红), On Legal Remedy of Impinged Right of Privacy (浅谈隐私权被侵犯的法律救济), in: Journal of Shanxi Politics and Law Institute for Administration (山西省政法管理干部学院学报), Vol. 17, No. 3, Taiyuan 2004, S. 20. Auch WANG Liming sieht personenbezogene Daten als Teil der Privatsphäre, gesteht ihnen jedoch auch die Qualität von (materiellem) Eigentum zu; vgl. hierzu *WANG Liming* (2005) (Fn. 55), S. 637; *Simon Werthwein* (Fn. 44), S. 83 f.

68 Vgl. *HU Weiping/ZHENG Jian* (胡卫萍/郑剑), On the Confirmed Civil Right of Personal Information Right (个人信息权民事确权刍议), in: Journal of East China Jiaotong University (华东交通大学学报), Vol. 27, No. 5, Nanchang 2010, S. 86.

69 Während der Schwerpunkt einer Rechtsverletzung der Privatsphäre in erster Linie auf dem immaterielle Schaden liegt, folgt aus dem Missbrauch personenbezogener Daten auch ein materieller Schaden; vgl. hierzu *HU Weiping/ZHENG Jian* (Fn. 61), S. 87.

70 Vgl. *HU Weiping/ZHENG Jian* (Fn. 61), S. 88.

71 Vgl. *HU Weiping/ZHENG Jian* (Fn. 61), S. 89.

72 Chin.: 个人信息权.

73 Vgl. *ZHANG Zhenliang* (Fn. 60), S. 42.

74 Vgl. *ZHANG Zhenliang* (Fn. 60), S. 43 ff.

75 Vgl. *Simon Werthwein* (Fn. 44), S. 83. SHEN/XU sehen Daten allerdings auch nach ihrer Veröffentlichung als vom Recht auf Privatsphäre geschützt an; vgl. *SHEN Che/XU Wenjie* (Fn. 55), S. 107 f.

76 Vgl. *WANG Liming* (2012) (Fn. 54), S. 112 f.

77 Bereits QI sieht personenbezogene Daten nicht als grundsätzlich unter die Privatsphäre fassbar und sieht daher einen Schutz personenbezogener Daten über ein allgemeines Persönlichkeitsrecht als notwendig an; vgl. *QI Aimin* (2004) (Fn. 55), S. 34 ff.

sen, sei das Recht auf den Schutz von personenbezogenen Daten auch als aktives Kontrollrecht zu betrachten, das es dem Betroffenen erlaubt zu bestimmen, wie seine personenbezogenen Daten genutzt werden sollen. WANG verweist dabei auf das deutsche Konzept des Rechts auf informationelle Selbstbestimmung. Er sieht eine definitorische Trennung beider Rechte als notwendig an, auch wenn eine überschneidungsfreie Abgrenzung nicht in jedem Falle gegeben sein wird.[78]

Verfolgt man die Diskussion zum Recht auf Privatsphäre und dem Schutz personenbezogener Daten in der chinesischen Literatur, lassen sich somit grundsätzlich zwei Grundhaltungen feststellen, die zum einen den Schutz personenbezogener Daten als Teil des Rechts auf Privatsphäre betrachten, zum anderen für ein eigenständiges Recht auf informationelle Selbstbestimmung oder Datenschutz zum Teil auf der Grundlage eines allgemeinen Persönlichkeitsrechts plädieren.

4.2 Historischer Abriss grundsätzlicher Entwicklungstendenzen im chinesischen Recht

Einen besonderen Einfluss auf die Entwicklung des chinesischen Rechts im Hinblick auf den Schutz von personenbezogenen Daten und die Privatsphäre hatten die *Renrou-Sousuo*-Fälle[79] der Jahre 2006 bis 2008, die dazu geführt haben, dass in der Rechtswissenschaft ein besonderes Augenmerk auf den Datenschutz im Internet gelegt wurde.[80] Aufgrund der speziellen Charakteristik dieses Phänomens, bei dem eine Gruppe von Bürgern Informationen über ein Individuum über das Internet zusammensucht und anschließend in einer diffamierenden und den Betroffenen schädigenden Weise verwendet und weiterverbreitet, galt es jedoch zunächst rechtliche Schutzmechanismen zu etablieren für den besonderen Fall, dass ein Bürger personenbezogene Daten eines Dritten über Dienstleistungen eines ISP verbreitet und so diesem Dritten Schaden zufügt.

Als Veranschaulichung der Charakteristik und Problematik der so genannten *Renrou-Sousuo*-Fälle sei hier kurz ein Fall aus dem Jahre 2006 beschrieben. Nach der Trennung eines Ehepaares hatte sich die Verlassene in den Tod gestürzt. Auf einer Online-Plattform tauchten später Anschuldigen gegen den Ex-Mann auf, die zu Diffamierungen und der Veröffentlichung seiner personenbezogenen Daten durch einzelne Internetaktivisten führten. Durch die Veröffentlichung der Daten kam es schließlich zu erheblichen Beeinträchtigungen des alltäglichen Lebens des Ex-Mannes: Er wurde belästigt, verlor seinen Job und sogar das Haus seiner Eltern wurde Beleidigungen beschmiert. Er verklagte daraufhin die Betreiber der Online-Plattform und forderte sie zur Löschung seiner Daten sowie zum Ersatz des ihm durch die Veröffentlichung der Daten entstandenen immateriellen Schadens.[81]

In der Folge wurde die Frage diskutiert nach der Haftung des ISP für Inhalte, die über seine Dienstleistungen übermittelt werden (Intermediärhaftung). In den entsprechenden Urteilen wurde ein Kompromiss gefunden, der die Schutzinteressen des Betroffenen und die wirtschaftlichen Interessen des ISP, der für den entstandenen Schaden höchstens indirekt als Verursacher in Frage kommt, ausbalancieren soll.[82] Eine vollständige Inhaltskontrolle ist jedenfalls für den ISP mit unverhältnismäßig hohen Kosten verbunden. Ein ISP ist daher nur nach Bekanntwerden einer Rechtsverletzung aufgefordert, innerhalb eines angemessenen zeitlichen Rahmens und entsprechend seiner technischen Möglichkeiten, die betreffenden rechtswidrigen Inhalte zu löschen bzw. den Zugriff auf diese Inhalte durch die Öffentlichkeit zu verhindern.[83] Mit den Urteilen wurde zudem erstmalig die Lesart durchbrochen, das Recht auf Privatsphäre als Teilbereich des Rechts am guten Ruf einzuordnen.[84]

Das 2010 in Kraft getretene DelHaftG kann als ein Resultat der genannten Diskussion betrachtet werden, wenn es die Grundlagen der Urteile der *Renrou-Sousuo*-Fälle bzgl. der Haftungsregelungen für ISP und der Einordnung des Rechts auf Privatsphäre als eigenständiges Persönlichkeitsrecht aufgreift.[85] Durch die erstmalige Aufnahme internetbezogener Vorschriften in ein Gesetz stellt das DelHaftG zudem einen Durchbruch im bisher nur verwaltungsrechtlich regulierten chinesischen Internetrecht dar.[86] Der deliktsrechtlich verankerte Schutz von personenbezogenen Daten setzt allerdings eine Verletzung des Rechts auf Privatsphäre sowie eine Schädigung des Betroffenen voraus. Als eine Ergänzung des privatrechtlichen Schutzes personenbezogener Daten lässt sich vor diesem Hintergrund der noch später zu untersuchende § 253-1 des 2009 zum siebten Male

---

78 Vgl. *WANG Liming* (2012) (Fn. 54), S. 119 f.

79 Chin.: 人肉搜索 – dt. etwa: „Menschenfleisch-Suche".

80 Zu zwei beispielhaft ausgewählten *Renrou-Sousuo*-Fällen vgl. *XUE Hong,* Privacy and personal data protection in China: An update for the year end 2009, in: Computer Law & Security Review, Vol. 26, Oxford 2010, S. 288; vgl. auch Fall 4.2 in *LUO Shenghua* (罗胜华), Analyse von Fallbeispielen zum Internetrecht (网络法案例评析), Beijing 2012, S. 92–97.

81 Vgl. *LUO Shenghua* (Fn. 72), S. 92 f.

82 Vgl. *XUE Hong* (Fn. 72), S. 288.

83 Vgl. *HU Ling* (胡凌), Reviews on Three First Trial Judgments of Human Powered Search Engine "First Case" (评人肉搜索“第一案”的三个初审判决), in: Internet Law Review (网络法律评论), Vol. 14, Beijing 2012, S. 183.

84 Vgl. *HU Ling* (Fn. 75), S. 181; vgl. hierzu die Ausführungen unter Punkt 5.1 bzw. 5.2.

85 Dies tut es in seinen §§ 2 Abs. 2 und 36; vgl. hierzu ausführlich Punkt 5.2.

86 HU betrachtet bereits die Urteile der *Renrou-Sousuo*-Fälle als einen solchen Durchbruch, da bereits sie das Recht auf Privatsphäre zu einem vollwertigen Persönlichkeitsrecht erklären; vgl. *HU Ling* (Fn. 75), S. 185.

revidierten StGB betrachten. Ob die Kodifizierung im StGB ebenfalls als eine Antwort auf die Renrou-Sousuo-Fälle zu sehen ist, ist allerdings zumindest fraglich.[87] Die Aufnahme einer Regelung zum Schutz personenbezogener Daten ins Strafrecht wird jedenfalls als Reaktion auf in der Vergangenheit vorgekommenen Missbrauchsfälle durch Behörden und Organisationen u.a. im Telekommunikations- und Bankensektor betrachtet.[88] Die Rechtsmaterie der beiden genannten Gesetzesnormen soll in den nächsten Abschnitten ausführlicher beleuchtet werden.

Parallel wurde im Jahr 2007 auf parlamentarischer Ebene eine Diskussion zur Einführung eines Datenschutzgesetzes in China initiiert. Auf der fünften Sitzung des zehnten Nationalen Volkskongresses (NVK) im Jahre 2007 und auf der ersten Sitzung des elften NVK ein Jahr später wurde bereits die Relevanz eines solchen Gesetzes erörtert.[89] Der Entwurf zu einem chinesischen Datenschutzgesetz von ZHOU Hanhua ist der umfassendste und daher in der Literatur am häufigsten zitierte. Einige Aspekte zu diesem und anderen Entwürfen sollen in den letzten Abschnitten dieses Beitrags genauer betrachtet werden.[90] Offenbar insbesondere vor dem Hintergrund des noch in Zukunft zu erlassenen Zivilgesetzbuches wurden jedoch anstelle eines umfassenden Datenschutzgesetzes bisher lediglich einzelne Regelungen in verschiedenen Gesetzen und Verordnungen umgesetzt,[91] so dass bis zum heutigen Zeitpunkt ein umfassendes und solides Regelungswerk zum Datenschutz fehlt.

Bereits vor 2009 wurden zudem vereinzelte branchenspezifische Regelungen zum Schutz von Privatsphäre und personenbezogenen Daten meist in Form von Verwaltungsrechtsbestimmungen erlassen.[92] Insbesondere sind hier im medizinischen Bereich die 1999 erlassenen Regelungen zum Schutz von Informationen über HIV-Patienten,[93] sowie der seit 2005 zunächst in Form einer brancheninternen Regelung,[94] später auch für andere Branchen kodifizierte Schutz von persönlichen Konto- und Kreditkartendaten[95] zu nennen. Auch in verschiedenen Gesetzen zu speziellen Rechtsbereichen finden sich Normen zum Schutz der Privatsphäre, z.B. im Jugendschutzgesetz von 1991, im Rechtsanwaltsgesetz von 1996, im Gesetz zu praktizierenden Medizinern von 1998, im Versicherungsgesetz von 2002, im Beglaubigungsgesetz von 2005 sowie im Geldwäschegesetz von 2006. Das Personalausweisgesetz von 2003 und das Passgesetz von 2006 enthalten zudem bereits Regelungen in Bezug auf personenbezogene Daten.[96] Der „Beschluss zum Schutz der Sicherheit im Internet" aus dem Jahr 2000 (SchutzIntSicherhBeschl) sieht eine strafrechtliche Verfolgung unter anderem für „den Diebstahl, das Verfälschen oder das Löschen von E-Mails oder anderem Datenmaterial Dritter"[97] vor, wenn eine Straftat nach dem StGB vorliegt. Da das StGB jedoch erst seit der Revision im Jahr 2009 Regelungen zum Schutz von personenbezogenen Daten enthält, ist fraglich, ob mit diesem „Datenmaterial" explizit auch einzelne Individualdaten gemeint sind.

Problematisch an der Regelungslage vor 2009 ist zum einen die nur spezialgesetzliche Normierung, die lediglich auf bestimmte Rechtssubjekte Anwendung findet und der zudem eine einheitliche definitorische Grundlage fehlt, zum anderen die Unterschiedlichkeit der verwendeten Begriffe in den Einzelnormen.[98] Die einzelnen Regelungen können daher keinen ausreichenden grundsätzlichen Schutz für personenbezogenen Daten bieten. Für den Bereich des Cloud-Computing sind die in diesem Abschnitt behandelten datenschutzrechtlichen Regelungen nur in wenigen rechtlich eng umrissenen Fällen anwendbar.

5. Schutz der Privatsphäre als Persönlichkeitsrecht

Bereits oben wurde festgestellt, dass ein Recht auf Privatsphäre nicht problemlos aus der chinesi-

---

87 Vgl. *SHEN Yuzhong* (沈玉忠), Personal Information Protection and the Legitimacy of Intervention by the Criminal Law—Comment on "Amendment on Criminal Law (七)" Clause 7 (个人信息保护与刑法干预的正当性——兼评《刑法修正案 (七)》第七条), in: Journal of Yanshan University (Philosophy and Social Sciences Edition) (燕山大学学报 (哲学社会科学版)), Vol. 10, No. 2, Qinhuangdao 2009, S. 86 f.

88 Vgl. *SHEN Yuzhong* (Fn. 79), S. 85.

89 Vgl. *XUE Hong* (Fn. 72), S. 287; „Ergebnisbericht des Rechtsausschusses des NVK zu vom Präsidium der 5. Sitzung des 10. NVK zur Untersuchung vorgelegten Vorschlägen von Delegierten" (全国人民代表大会法律委员会关于第十届全国人民代表大会第五次会议主席团交付审议的代表提出的议案审议结果的报告) vom 29. Dezember 2007 (NVK-RA 2007), Gazette of the Standing Committee of the National People's Congress of the People's Republic of China (中华人民共和国全国人民代表大会常务委员会公报), No. 1, Peking 2008, S. 158–171, Anhang: Punkt III 21/22/23; „Ergebnisbericht des Rechtsausschusses des NVK zu vom Präsidium der 1. Sitzung des 11. NVK zur Untersuchung vorgelegten Vorschlägen von Delegierten" (全国人民代表大会法律委员会关于第十一届全国人民代表大会第一次会议主席团交付审议的代表提出的议案审议结果的报告) vom 27. Dezember 2008 (NVK-RA 2008), Gazette of the Standing Committee of the National People's Congress of the People's Republic of China (中华人民共和国全国人民代表大会常务委员会公报), No. 1, Peking 2013, S. 133–141, Anhang: Punkt IV 20.

90 S. dazu ausführlich Punkt 11.1 und 11.2.

91 Vgl. NVK-RA 2008, Anhang: Punkt IV 20.

92 Es sei an dieser Stelle betont, dass in diesem Artikel auf einzelne branchenspezifische Regelungen zum Datenschutz, wie sie bspw. für den Bankensektor, Versicherungen, Rechtsanwälte oder Ärzte existieren, nicht eingegangen werden kann.

93 „Ansichten zur Verwaltung von HIV-Infizierten und AIDS-Patienten" (关于对艾滋病病毒感染者和艾滋病病人的管理意见).

94 „Einstweilige Verwaltungsbestimmungen für Basis-Datenbanken für persönliche Kreditinformationen" (个人信用信息基础数据库管理暂行办法).

95 Vgl. *HONG Hailin* (Fn. 4), S. 156.

96 Vgl. *HONG Hailin* (Fn. 4), S. 155 f.

97 § 4 Abs. 2 „Beschluss des Ständigen Ausschusses des NVK zum Schutz der Sicherheit im Internet" (全国人民代表大会常务委员会关于维护互联网安全的决定) vom 28. Dezember 2000 (SchutzIntSicherhBeschl), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 5, Peking 2001, S. 21–23.

98 So wird zum Teil der „Schutz der Privatsphäre" (隐私保护) vorgeschrieben, zum Teil wird das „Veröffentlichen der persönlichen Privatsphäre" (泄露个人隐私) verboten.

schen Verfassung ableitbar ist. Nicht zuletzt auch aufgrund der ebenfalls bereits oben angesprochenen historischen Entwicklung sind jedoch im Privatrecht Entwicklungen eines Schutzes der Privatsphäre über den Weg der Rechtspositivierung festzustellen. Bevor die aktuellen Rechtsgrundlagen für den Schutz der Privatsphäre und der persönlichen Daten zur Anwendung für den Diskussionsgegenstand analysiert werden sollen, soll im Folgenden die Herausbildung des Rechts auf Privatsphäre im Privatrecht näher beleuchtet werden.

5.1 Herausbildung des Rechts auf Privatsphäre über die AGZ

In den 1986 erlassenen „Allgemeinen Grundsätze des Zivilrechts" (AGZ) findet sich zunächst ein grundsätzlicher Schutz von gesetzlich verbürgten Rechten natürlicher und juristischer Personen,[99] es wird jedoch kein Recht auf Privatsphäre, sondern neben dem Recht am eigenen Namen[100] und am eigenen Bildnis[101] in § 101 ausdrücklich lediglich das Recht am guten Ruf[102] definiert. Nach § 101 AGZ genießt dabei „die Achtung vor der Persönlichkeit des Bürgers […] den Schutz des Gesetzes, und es ist verboten mit Mitteln wie denen der Beleidigung und Verleumdung den Ruf von Bürgern […] zu schädigen."[103]

Wenngleich in den AGZ selbst das Recht auf Privatsphäre nicht explizit genannt wird, ist jedoch ein konkreter Bezug zum Schutz der Privatsphäre in den „(testweise durchgeführten) Ansichten des OVG zu einigen Fragen bezüglich der Durchführung der AGZ" von 1988 zu finden, wo es heißt, dass die schriftliche wie mündliche Preisgabe der Privatsphäre Dritter, soweit dies das Recht des Betroffenen an seinem Ruf in einem bestimmten Grade schädigt, mit der Verletzung des Rechts am guten Ruf gleichzusetzen ist.[104] Mit dieser Interpretation hat der OVG erstmalig die Existenz eines Rechts auf Privatsphäre festgestellt und Bürgern unter bestimmten Voraussetzungen den Schutz dieses Rechts zuerkannt.[105] In den „Erläuternden Antworten des OVG auf einige Fragen bezüglich der Behandlung von Fällen zum Recht am guten Ruf" von 1993 bestätigt das Gericht zudem seine „Ansichten" von 1988 und ergänzt sie insofern, als neben der schriftlichen wie mündlichen Preisgabe der Privatsphäre Dritter auch die Veröffentlichung „privater Dokumente"[106] ohne Zustimmung des Betroffenen eine deliktische Handlung darstellt, die das Recht auf Privatsphäre Dritter verletzt.[107]

Es bleibt festzuhalten, dass es sich bei dem Schutz der Privatsphäre in der vorstehenden Form um einen speziellen Schutz des Rechts am guten Ruf handelt, der lediglich im Falle einer Rechtsverletzung greift und nur bei einem nachweisbaren Schaden zivilrechtliche Folgen nach sich zieht. In der Literatur wird daher bereits die 1988er Entscheidung des OVG insofern kritisiert, als sie das Recht auf Privatsphäre dem Recht am guten Ruf unterordnet.[108] Ein grundsätzlicher Schutz der Privatsphäre, genauso wenig wie eine umfassende Definition des Schutzbereiches, ist jedenfalls auf diese Weise nicht gegeben.

Die Problematik des nachweisbaren Schadens, der dem Betroffenen durch die Preisgabe von privaten Informationen entsteht, besteht insbesondere deswegen, weil im chinesischen Recht lange Zeit das Konzept des immateriellen Schadens nur unzureichend kodifiziert war. Immerhin sehen die AGZ für die Verletzung des Rechts am Namen, am Bildnis, am guten Ruf und an der Ehre unter anderem die Wiederherstellung des Rufs und eine Entschuldigung vor.[109] Eine grundlegende Änderung brachten die „Erklärungen des OVG zu einigen Fragen bezüglich der Bestimmung der zivilen deliktischen Haftung für Entschädigungen von immateriellen Schäden" von 2001, die für die Verletzung unter anderem des Rechts am guten Ruf auch einen Entschädigungsanspruch für immaterielle Schäden (wörtlich: „seelische Schäden"[110]), also einen Anspruch auf Schmerzensgeld, vorsehen.[111]

Bemerkenswert ist die Tatsache, dass in den Erklärungen von 2001 neben einer Aufzählung von Persönlichkeitsrechten, für die die Anerkennung eines solchen immateriellen Schadens in Frage kommt, in einem weiteren Untersatz gesondert definiert wird, dass ein immaterieller Schaden unter

---

99 Vgl. § 5 „Allgemeine Grundsätze des Zivilrechts der VR China" (中华人民共和国民法通则) vom 12. April 1986 (AGZ), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 12, Peking 1986, S. 371–393.

100 S. § 99 AGZ.

101 S. § 100 AGZ.

102 Chin.: 名誉权.

103 § 101 AGZ; vgl. *SHEN Che/XU Wenjie* (Fn. 55), S. 263.

104 Vgl. Nr. 140 AGZAns; *MA Yichan* (Fn. 52), S. 39.

105 Vgl. *SHEN Che/XU Wenjie* (Fn. 55), S. 263.

106 Chin.: 隐私材料.

107 Vgl. Nr. 7 „Erläuternde Antworten des OVG auf einige Fragen bezüglich der Behandlung von Fällen zum Recht am guten Ruf" (最高人民法院关于审理名誉权案件若干问题的解答) vom 15. Juni 1993 (RufReAntw), Gazette of the Supreme People's Court of the People's Republic of China (中华人民共和国最高人民法院公报), No. 3, Peking 1993, S. 102–103. Der OVG hat 1998 die RufReAntw noch einmal ergänzt, außer einer speziellen Regelung, die die Privatsphäre von Patienten betrifft, sind jedoch keine neuen die Privatsphäre oder personenbezogene Daten betreffenden Interpretationen aufgenommen worden.

108 Vgl. *WU Yanfen/MA Qinghong* (Fn. 60), S. 19.

109 Vgl. § 120 AGZ.

110 Chin.: 精神损害.

111 Vgl. § 1 „Erläuterungen des OVG zur Feststellung einiger Fragen bezüglich der zivilen Haftung von immateriellen Schäden" (最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释) vom 26. Februar 2001 (ZivHaftErkl), Gazette of the Supreme People's Court of the People's Republic of China (中华人民共和国最高人民法院公报), No. 2, Peking 2001, S. 51–52.

anderem auch dann vorliegt, wenn die Verletzung der Privatsphäre einen Verstoß „gegen die gesellschaftlichen öffentlichen Interessen oder die gesellschaftliche öffentliche Moral“[112] darstellt.[113] Dies legt die Vermutung nahe, dass nicht unbedingt das Recht am guten Ruf (oder ein anderes aufgeführtes Persönlichkeitsrecht) verletzt worden sein muss, damit eine Entschädigung auf Grundlage einer Verletzung des Rechts auf Privatsphäre möglich ist, sondern eine Verletzung des Rechts auf Privatsphäre auch direkt als Klagegrund angeführt werden kann.[114] Zumindest ist ein direkter Schutz der Privatsphäre durch die „Erklärungen“ gegeben, auch wenn auf dieser Grundlage der Schutz der Privatsphäre nicht als Persönlichkeitsrecht einzustufen ist.[115]

5.2 Deliktsrechtlicher Schutz des Rechts auf Privatsphäre

Mit dem DelHaftG von 2009 wird das Recht auf Privatsphäre zum ersten Mal als generelles geschütztes Rechtsgut in einem chinesischen Gesetz aufgeführt.[116] Im DelHaftG wird dieses Recht ausdrücklich neben den Rechten u.a. am eigenen Namen, am guten Ruf, an der Ehre und am eigenen Bildnis privatrechtlich als Persönlichkeitsrecht definiert,[117] womit die bisher als problematisch kritisierte Subsumierung unter das Recht am guten Ruf endgültig aufgehoben wird.[118] Als Formen der Haftung bei Rechtsverletzung sind nach § 15 DelHaftG unter anderem Unterlassung der Rechtsverletzung, Beseitigung von Behinderungen, Rückgewähr von Vermögensgütern, Entschuldigung und Haftung bei Nachwirkungen definiert.[119] Des weiteren umfasst der Schadenersatz sowohl Vermögensschäden als auch Nichtvermögensschäden in Form eines Schmerzensgeldes[120] insofern, als eine Entschädigung erfolgen kann, wenn ein „erheblicher“ immaterieller Schaden durch die Verletzung von zivilen Rechten entstanden ist.[121] ZHENG/Trempel kritisieren, dass das notwendige Ausmaß des Schadens nicht näher konkretisiert wird.[122] Zudem ist strittig, ob bei bereits zuerkanntem materiellen Schadensersatz ein weitergehender immaterieller Schadensersatz eingeklagt werden kann.[123] Das grundsätzliche bisher existente Problem jedenfalls, dass eine Verletzung der Privatsphäre aufgrund der Ableitung des Rechts auf Privatsphäre aus dem Recht am guten Ruf nur dann vorliegen konnte, wenn dem Betroffenen ein Schaden an seinem gesellschaftlichen Ruf entstanden ist, wird durch die Formulierung des Rechts auf Privatsphäre als eigenständiges Persönlichkeitsrecht ausgeräumt.[124]

Aufgrund der Vagheit des Begriffs der Privatsphäre ist eine Konkretisierung wünschenswert, jedoch findet sich diese im DelHaftG selbst nicht.[125] Es stellt sich andererseits die Frage, ob eine solche Konkretisierung ins DelHaftG hineingehört oder nicht vielmehr in den allgemeinen Teil eines in Zukunft zu erlassenen Zivilgesetzbuches, zu dessen besonderen Teilen das DelHaftG zweifelsohne gehören wird. Mit der Aufnahme des Rechts auf Privatsphäre ins DelHaftG ist jedenfalls auch weiterhin die Privatsphäre nur dann geschützt, wenn der Betroffene einen Schaden durch einen (zivilen) Dritten erleidet.

5.3 Besondere Haftungsregelungen für Internetnutzer und ISP

Das DelHaftG enthält in § 36 besondere Regelungen für Internetnutzer und ISP, die i.V.m. § 2 Abs. 2 DelHaftG auch Relevanz für den Schutz der Privatsphäre aufweisen. Zunächst wird ausdrücklich hervorgehoben, dass „Internetnutzer und ISP[126], die über das Internet die Rechte Dritter verletzen, […] die zivile Haftung übernehmen“[127]. Dass der Gesetzgeber die besondere Situation der Rechtsverletzung im Internet hier hervorhebt, ist offenbar auch im Zusammenhang mit den o.g. *Renrou-Sousuo*-Fällen zu sehen, da eine deliktische Handlung regelmäßig die zivile Haftung durch Verschulden bereits nach § 6 DelHaftG nach sich zieht. Allerdings fordern Besonderheiten von deliktischen Handlungen im Internet auch eine besondere Betrachtung der Haftungsregelungen.[128] § 36 Abs. 1 DelHaftG regelt zunächst die Haftung von Internetnutzern bzw. ISP

---

112 § 1 Abs. 2 ZivHaftErkl.

113 Vgl. *SHEN Che/XU Wenjie* (Fn. 55), S. 264.

114 Vgl. *SHEN Che/XU Wenjie* (Fn. 55), S. 264.

115 Vgl. Simon Werthwein (Fn. 44), S. 85.

116 Das Recht wird jedoch bereits in § 42 des vier Jahre früher erlassenen Gesetzes zur Sicherung der Rechte und Interessen von Frauen (中华人民共和国妇女权益保障法) erwähnt, wo es schlicht heißt, dass Persönlichkeitsrechte von Frauen, zu denen auch das Recht auf Privatsphäre gezählt wird, rechtlichen Schutz genießen. Der Begriff der Privatsphäre wird immerhin bereits seit 1986 in verschiedenen Spezialgesetzen (u.A. zur Gerichtsorganisation, zum Jugendschutz oder zum Verwaltungsprozess) erwähnt; vgl. hierzu auch *SHEN Che/XU Wenjie* (Fn. 55), S. 263.

117 Vgl. § 2 Abs. 2 DelHaftG.

118 Zur Gleichrangigkeit der einzelnen Persönlichkeitsrechte im DelHaftG vgl. auch *WANG Liming* (2012) (Fn. 54), S. 112.

119 Vgl. § 15 DelHaftG; *ZHENG Shuji/Eberhard J. Trempel,* Das (neue) Delikthaftungsrecht der VR China, in: Recht der Internationalen Wirtschaft, Heft 8, Frankfurt am Main 2010, S. 519.

120 Vgl. *ZHENG Shuji/Eberhard J. Trempel* (Fn. 108), S. 520.

121 Vgl. § 22 DelHaftG.

122 Vgl. *ZHENG Shuji/Eberhard J. Trempel* (Fn. 108), S. 520.

123 Vgl. *XU Yan* (徐燕), Die Delikthaftungsgesetzgebung: Sorgfältiger Schutz des Volkswohls – WANG Shengming, Vertreter des Gesetzgebungsausschusses des ständigen Ausschusses des Nationalen Volkskongresses, zum rechtlichen System der deliktischen Haftung (侵权责任立法: 精心呵护民生——全国人大常委会法工委副主任王胜明谈侵权责任法律制度), in: The People's Congress of China (中国人大), Vol. 14, Beijing 2009, S. 25.

124 Vgl. *WU Yanfen/MA Qinghong* (Fn. 60), S. 19.

125 Vgl. aber zu den Definitionen in der Literatur Punkt 4.1.

126 Chin.: 网络服务提供者.

127 § 36 Abs. 1 DelHaftG.

128 Vgl. *WANG Shengming* (Fn. 56), S. 188.

für selbstverschuldete Rechtsverletzungen Dritter. Neben Rechtsverletzungen im Bereich des Vermögens- bzw. Immaterialgüterrechts sind hier auch Verletzungen von Persönlichkeitsrechten miteingeschlossen.[129]

Eine genauere Definition des ISP liefert das DelHaftG nicht. Für die Anwendung im vorliegenden Fall sieht WANG Shengming eine Differenzierung des allgemeinen Begriffs des Internetdienstanbieter in technische und inhaltliche Dienstanbieter[130] als notwendig an und betrachtet den Schwerpunkt der Regelungen in § 36 DelHaftG auf dem technischen Dienstanbieter liegend.[131] Obgleich die Meinungen einzelner Experten bei der Frage differieren, welche Formen der Dienstleistung von § 36 DelHaftG konkret umfasst sind, kann aufgrund des diesbezüglich relativ einhelligen Standpunktes in der chinesischen Literatur als h.M. angesehen werden, dass jedenfalls auf Anbieter von Datenspeicherplatz, von Suchmaschinen sowie von Link-Aggregationsdiensten § 36 DelHaftG anzuwenden ist.[132] Damit ist § 36 DelHaftG jedenfalls auch auf Anbieter von Cloud-Diensten anwendbar.

Während § 36 Abs. 1 DelHaftG nur Rechtsverletzungen aufgrund von eigenen Inhalten des ISP bzw. Internetnutzers betrifft und damit für Cloud-Dienstleistungen, die in erster Linie fremde Inhalte verarbeiten, weniger Relevanz aufweist, finden sich in den §§ 36 Abs. 2 und Abs. 3 DelHaftG weitere besondere Regelungen, die die Haftung des ISP auch für fremde Inhalte regeln. Es heißt dort, dass „[w]enn Internetnutzer vermittels eines Internetdienstes[133] eine deliktische Handlung vollziehen, der Geschädigte [nach § 36 Abs. 2 DelHaftG] das Recht [hat], den ISP um eine Löschung oder Sperrung [der betreffenden Inhalte], eine Aufhebung der Verlinkung oder die Ergreifung vergleichbarer notwendiger Maßnahmen zu ersuchen. Der ISP haftet gemeinsam mit dem Internetnutzer [d.h. mit dem Schädiger] gesamtschuldnerisch, wenn er nicht nach dem Ersuchen [durch den Geschädigten] unverzüglich die entsprechenden notwendigen Maßnahmen ergreift“[134]. Weiter heißt es in § 36 Abs. 3 DelHaftG, dass ein „ISP [auch dann] gemeinsam mit dem Internetnutzer gesamtschuldnerisch [haftet], wenn er weiß, dass dieser Internetnutzer über die Nutzung seiner Dienste die zivilen Rechte Dritter schädigt, und er keine entsprechenden notwendigen Gegenmaßnahmen ergreift“[135].

Das DelHaftG steht mit der Anwendung der gesamtschuldnerischen Haftung bei Rechtsverletzungen aufgrund von Inhalten im Internet in der Tradition der „Erläuterungen des OVG zur Behandlung einiger Fragen bezüglich der Anwendung von Gesetzen in Streitigkeiten das Urheberrecht in elektronischen Netzwerken betreffend“ (UrhReErl) von 2000 (2006 revidiert), die eine gesamtschuldnerische Haftung von Schädiger und ISP nach § 130 AGZ vorsehen, wenn der ISP den Schädiger zu einer deliktischen Handlung angestiftet, ihm geholfen oder an der Tat selbst beteiligt war[136] oder wenn der ISP trotz Inkenntnissetzung durch den Geschädigten keine Gegenmaßnahmen zur Verhinderung von weiteren Rechtsverletzungen getroffen hat.[137] Das DelHaftG weitet diese Anwendung nun jedoch verallgemeinernd auf Verletzungen von Persönlichkeitsrechten aus. Ob das Konstrukt der gesamtschuldnerischen Haftung in diesem Falle eine Abweichung vom Grundsatz der Verschuldenshaftung darstellt, wird in der Literatur kritisch diskutiert.[138] Bemängelt wird insbesondere, dass der ISP unter Umständen bereits durch eine Unterlassung haftbar gemacht werden kann. Allerdings beschränkt sich seine Haftung auf Schäden, die durch die Unterlassung der Entfernung der entsprechenden rechtsverletzenden Informationen entstanden sind.[139]

Ebenfalls bereits in den UrhReErl findet sich eine Bestimmung zur „Mitteilung zur Entfernung“[140], die dem Geschädigten das Recht gibt, den ISP über die Rechtsverletzung in Kenntnis zu setzen und ihn aufzufordern, die Rechtsverletzung durch entsprechende Maßnahmen zu beseitigen.[141] Auch die „Bestimmungen der VR China zum Schutz des Rechts auf Kommunikation in Datennetzwerken“ von 2006 (KommReBest) kennen bereits eine solche Regelung, hier hat die Meldung ausdrücklich in schriftlicher Form zu erfolgen[142] und der ISP nach

---

129 Vgl. *WANG Shengming* (Fn. 56), S. 191.

130 Chin.: 技术服务提供者 bzw. 内容服务提供者.

131 Vgl. *WANG Shengming* (Fn. 56), S. 189. Zu Bemerken ist allerdings, dass zumindest § 36 Abs. 1 DelHaftG grundsätzlich auch auf ISP, die eigene Inhalte anbieten, zur Anwendung kommen kann. Zur begrifflichen Definition des Internetdienstanbieters s. auch Punkt 9.1.

132 Vgl. *WANG Shengming* (Fn. 56), S. 189; vgl. auch *HE Jian* (贺剑), Analysis on Internet Tort System from the Perspective of Tort Law (侵权责任法视野下的网络侵权制度), in: Internet Law Watch (互联网法律通讯), Vol. 6, No. 2, Beijing 2010, S. 55.

133 Chin.: 网络服务.

134 § 36 Abs. 2 DelHaftG.

135 § 36 Abs. 3 DelHaftG.

136 Vgl. § 3 „Erläuterungen des OVG zur Behandlung einiger Fragen bezüglich der Anwendung von Gesetzen in Streitigkeiten das Urheberrecht in elektronischen Netzwerken betreffend“ (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释) vom 22. November 2000 (in der revidierten Fassung vom 20. November 2006 (UrhReErl), New Laws and Regulations Monthly (新法规月刊), No. 4, Shanghai 2006, S. 86–87.

137 Vgl. § 4 UrhReErl; vgl. zu beiden Regelungen auch *WANG Shengming* (Fn. 56), S. 186 f. und 188.

138 Vgl. *Jörg Binding,* Das Gesetz der VR China über die deliktische Haftung, Berlin 2012, S. 75.

139 Vgl. *HE Jian* (Fn. 119), S. 56.

140 In der Literatur wird dieser Mechanismus in Anlehnung an das US-amerikanische Digital Millennium Copyright Act als „通知与取下“ bzw. „notice and take-down“ bezeichnet.

141 Vgl. § 4 UrhReErl.

142 Vgl. § 14 „Bestimmungen der VR China zum Schutz des Rechts auf

Erhalt der Meldung umgehend entsprechende Maßnahmen zu ergreifen.[143] Die Regelung existiert nun im DelHaftG fort. Die Tatsache, dass der ISP haftet, wenn er von einer Rechtsverletzung, die über seinen Dienst verübt wurde, „weiß" und nichts dagegen unternimmt, wird in der erläuternden Literatur so verstanden, dass „wissen"[144] als vergleichsweise neutrale Begrifflichkeit hier sowohl „sicher wissen"[145], eher perfektiv zu verstehen, als auch „wissen sollen"[146], mit einer obligatorischen Konnotation, umfasst.[147] Die Forderung, dass der ISP in einer konkreten Situation das Vorhandensein einer entsprechenden Rechtsverletzung hätte „wissen sollen", ist jedoch stets schwierig durchzusetzen, weswegen der durch die neutralere Begriffswahl entstehende Interpretationsspielraum durchaus als gewollt zu betrachten ist.[148]

Auf den Gegenstand des Cloud-Computing bezogen lässt sich zunächst sagen, dass Anbieter von Cloud-Diensten unter den hier verwendeten Begriff des ISP einzuordnen sind und folglich im Sinne des § 36 DelHaftG die zivile Haftung übernehmen. Als deliktische Handlung gilt auch die Verletzung des Rechts auf Privatsphäre eines Dritten nach § 2 Abs. 2 DelHaftG. Damit haftet ein Anbieter eines Cloud-Dienstes für Delikte, die er selbst über das Internet verübt hat, direkt, sowie für Delikte, die ein Nutzer seiner Dienste verübt hat, gemeinsam mit diesem gesamtschuldnerisch, wenn er von diesen Rechtsverletzungen – aus eigenem Antrieb oder durch Hinweis des Geschädigten – Kenntnis erlangt hat, jedoch keine erforderlichen Maßnahmen zur Verhinderung von weiteren Rechtsverletzungen ergreift. Das DelHaftG spricht in allgemeiner Form von dem „Dritten" bzw. „Geschädigten".[149] Daher sind auch Rechtsverletzungen von Personen, die mit dem ISP und Internetnutzer nur indirekt in Verbindung stehen (beispielsweise Mitarbeiter oder Kunden eines Unternehmens, das selbst wiederum Kunde des Cloud-Dienstleisters ist), durch die genannten Regelungen grundsätzlich abgedeckt.

Die Tatsache, dass das Recht auf Privatsphäre kein direktes verfassungsmäßiges Grundrecht ist, sowie der fehlende Schutz der Privatsphäre als solche im Strafrecht und die ausschließliche Erwähnung im DelHaftG lassen darauf schließen, dass sich das Recht auf Privatsphäre zwar über die verfassungsmäßigen Grundrechte auf den Schutz der persönlichen Würde, den Schutz der Wohnung und das Geheimnis der Korrespondenz begründen lässt, selbst jedoch hier nur eine privatrechtliche Funktion entfalten kann.[150] WANG Liming kritisiert, dass die Berücksichtigung des Rechts auf Privatsphäre im DelHaftG nicht für einen umfassenden Schutz der Privatsphäre genügt, da das Recht auf Privatsphäre nicht definiert, sondern nur genannt wird. Sein Umfang und Inhalt sind damit unklar und bedürfen einer weiteren Konkretisierung. Abgesehen davon ist es die Funktion des DelHaftG, dem durch eine Rechtsverletzung Geschädigten Rechtsmittel zur Hand zu geben, nicht aber, Rechte allgemein zu definieren oder zu schützen.[151]

Es ist festzuhalten, dass das Recht auf Privatsphäre jedenfalls nicht mit einem ausreichenden Datenschutz im Sinne eines Rechts auf informationelle Selbstbestimmung gleichzusetzen ist. Durch die Subsumierung des Schutzes personenbezogener Daten unter das Recht auf Privatsphäre kann hier der Datenschutz nur insofern greifen, als eine Verletzung der Privatsphäre gegeben ist.[152] Für eine Rechtsverletzung, aus der einem Datensubjekt Rechtsansprüche erwachsen, muss daher grundsätzlich eine rechtswidrige Handlung vorliegen, ein Schaden entstanden sein und ein Kausalzusammenhang zwischen Handlung und Schaden erkennbar sein. Aufgrund der gesamtschuldnerischen Regelung ist ein Verschulden des ISP jedenfalls nicht vom Betroffenen nachzuweisen. Dennoch ist eine solche Konstruktion über das Deliktsrecht einem umfassenden Datenschutz vermutlich wenig zuträglich, auch wenn freilich ein gewisser Schutz nicht von der Hand zu weisen ist.

6. Schutz von personenbezogenen Daten in Gesetzesnormen

6.1 Strafrechtlicher Schutz von personenbezogenen Daten

Der chinesische Gesetzgeber hat den Schutz von Privatsphäre und personenbezogenen Daten nicht ausschließlich im Zivilrecht kodifiziert. In der siebten Änderung des StGB aus dem Jahr 2009 findet sich erstmalig auch in diesem Rechtsbereich eine Formulierung zum Datenschutz: In § 253-1 StGB wird es Mitarbeitern von Staatsorganen sowie von Finanz-, Telekommunikations-, Verkehrs-, Bildungs- und medizinischen Einrichtungen verboten, persönliche Daten von Bürgern, die bei der

Kommunikation in Datennetzwerken" (信息网络传播权保护条例) vom 10. Mai 2006 (KommReBest), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 19, Peking 2006, S. 13–16.

143 Vgl. § 15 KommReBest.

144 Chin.: 知道.

145 Chin.: 明知.

146 Chin.: 应知.

147 Vgl. *WANG Shengming* (Fn. 56), S. 195.

148 Vgl. *HE Jian* (Fn. 119), S. 61 f.

149 Vgl. § 36 DelHaftG.

150 Vgl. *WANG Liming* (2012) (Fn. 54), S. 110 f.

151 Vgl. *WANG Liming* (2012) (Fn. 54), S. 114.

152 Vgl. *FU Xia* (付霞), Über die rechtlichen Regelungen der Kommodifizierung von personenbezogenem Datenmaterial im Cloud-Computing-Zeitalter (论云计算时代个人信息资料商品化的法律规制), in: Journal of Jilin Radio and TV University (吉林广播电视大学学报), No. 12, Changchun 2012, S. 110.

Ausübung ihrer Dienstpflichten erlangt wurden, zu verkaufen oder illegal an Dritte weiterzugeben. Eine Sanktion ist jedoch nur in „schwerwiegenden Fällen“[153] in Form einer Geldstrafe unter Umständen in Verbindung mit einer bis zu dreijährigen Haftstrafe vorgesehen.[154] In gleicher Weise ist der Diebstahl oder die illegale Aneignung der in Satz 1 genannten Daten verboten, auch hier ist eine entsprechende Sanktionierung nur in „schwerwiegenden Fällen“ vorgesehen.[155] Die Sanktionen richten sich sowohl gegen die verantwortliche Stelle als auch gegen die verantwortlichen Mitarbeiter dieser Stelle.[156] Eine Konkretisierung des Umfangs eines „schwerwiegenden Falles“ findet sich nicht.[157] ZHANG Lei fasst die verschiedenen Meinungen in der wissenschaftlichen Diskussion unter zwei Grundansätzen zusammen, die einmal von dem Ausmaß der Schädigung der Rechte des Betroffenen und einmal von der Verwendungsabsicht der Daten ausgehen.[158]

DIAO/ZHANG sehen in der aktuellen Regelung zum strafrechtlichen Schutz von personenbezogenen Daten das Problem, dass das Rechtssubjekt auf Mitarbeiter von Behörden sowie von Unternehmen weniger bestimmter Branchen begrenzt ist. Daten können jedoch nicht nur von diesem eng abgesteckten Personenkreis an Dritte weitergegeben werden, sondern prinzipiell von jedem.[159] In einem Gerichtsurteil, das einen Fall betraf, in dem personenbezogene Daten illegal veröffentlicht worden waren, wurde die Frage aufgeworfen, ob es sich in dem konkreten Fall überhaupt um eine Situation handelte, die von dem entsprechenden Paragraphen abgedeckt sei. Der Beklagte habe die Daten unter anderem weder „im Rahmen der Erfüllung öffentlicher Aufgaben“ noch „im Rahmen der Erbringung einer Dienstleistung“ erlangt, wie es aber § 253-1 Abs. 1 StGB vorsah.[160]

HUANG sieht die spezielle Formulierung des § 253-1 StGB darin begründet, dass der Gesetzgeber hier insbesondere solche Daten besonders schützen will, die aufgrund von anderen Vorschriften durch öffentliche Organe oder durch Unternehmen, die Dienstleistungen mit gewissen öffentlichen Funktionen anbieten und deswegen von bestimmten Regelungen betroffen sind, obligatorisch erhoben werden. Auf diese Weise befinden sich diese öffentlichen Organe oder Unternehmen gegenüber den Bürgern oder Kunden in einer stärkeren Position, in der sie vergleichsweise einfach bestimmte personenbezogene Daten erheben können. Daher sei, so HUANG, ein besonderer Schutz solcher personenbezogener Daten vorgesehen, deren Angabe unter Umständen zwingend notwendig ist, was sich in der Formulierung des entsprechenden Paragraphen widerspiegelt, der nur solche persönlichen Daten umfasst, die „im Rahmen der Erfüllung öffentlicher Aufgaben“ oder „im Rahmen der Erbringung einer Dienstleistung“ von Behörden oder Unternehmen der angegebenen Branchen erhoben wurden.[161] Andererseits ist möglicherweise die strafrechtliche Kodifizierung als Ansinnen des Gesetzgebers zu verstehen, einen Datenschutz unabhängig von einer Verletzung des Rechts auf Privatsphäre zu realisieren. Allerdings widerspricht dieser These ZHANG Mingkai, nach dessen Ansicht eben lediglich solche Daten einen strafrechtlichen Schutz genießen sollen, die die Privatsphäre des Bürgers betreffen, was den Namen, das Geschlecht und Angaben zur Erwerbstätigkeit ausschließt.[162] An anderer Stelle und auch in Gerichtsurteilen werden jedoch jegliche zur Identifizierung von Bürgern geeignete Daten, unabhängig von deren Bezug zur Privatsphäre des Bürgers, als persönliche Daten betrachtet, also auch Name und Arbeitsverhältnis oder Kontaktdaten wie beispielsweise Telefonnummern.[163]

DIAO/ZHANG sehen des weiteren ein Problem in dem nur symptomatischen Verbot des Verkaufs bzw. der anderweitigen rechtswidrigen Weitergabe von personenbezogenen Daten. Vielmehr sei bereits das rechtswidrige Erheben, Verarbeiten und Löschen von personenbezogenen Daten strafrechtlich zu sanktionieren. Zudem sei das Rechtsobjekt zu eng gefasst:[164] Der strafrechtliche Schutz greift nur

---

153 Chin.: 情节严重.

154 Vgl. § 253-1 Abs. 1 StGB.

155 Vgl. § 253-1 Abs. 2 StGB.

156 Vgl. § 253-1 Abs. 3 StGB.

157 Vgl. *CHANG Qing/ZHANG Li* (常青/张莉), Analyse der juristischen Anwendung des Tatbestandes der illegalen Aneignung von persönlichen Daten von Bürgern (非法获取公民个人信息罪司法适用之解构分析), in: Legal System and Society (法制与社会), Vol. 12 II, Kunming 2012, S. 88.

158 Vgl. *ZHANG Lei* (张磊), Probleme der Rechtsanwendung von Straftaten mit Bezug zu persönlichen Daten und ihre Gegenmaßnahmen (司法实践中侵犯公民个人信息犯罪的疑难问题及其对策), in: Contemporary Law Review (当代法学), Vol. 1, Changchun 2011. S. 77. Zhang Lei gibt zudem eine Reihe konkreter Beispiele für die Bestimmung eines „schwerwiegenden Falles“ für § 253-1 Abs. 1 und Abs. 2 StGB.

159 Vgl. *DIAO Shengxian/ZHANG Qiangqiang* (刁胜先/张强强), Personal Information and the Protection of Criminal Law in the Perspective of Cloud-Computing (云计算视野的个人信息与刑法保护), in: Chongqing Social Sciences (重庆社会科学), Vol. 4, Chongqing 2012, S. 49.

160 Vgl. *JIANG Ge,* Datenschutzrecht in China: heute und morgen, in: Datenschutz und Datensicherheit, Nr. 9, Wiesbaden 2011, S. 645.

161 Vgl. *HUANG Taiyun* (黄太云), Erklärungen zur „siebten Änderung des Strafgesetzbuches“ (《刑法修正案 (七)》解读), in: People's Procuratorial Semimonthly (人民检察), Vol. 6, Beijing 2009, S. 15. Damit stünden die genannten strafrechtlichen Regelungen konzeptionell in der Tradition der „Bestimmungen zur Veröffentlichung von Regierungsinformationen“ (政府信息公开条例), die grundsätzlich eine Veröffentlichung von Informationen, die die Privatsphäre von Einzelpersonen betreffen, durch Behörden untersagen.

162 Vgl. *ZHANG Mingkai* (张明楷), Criminal Law (刑法学), 4. Auflage, Beijing 2011, S. 824 f.

163 Vgl. *CHANG Qing/ZHANG Li* (Fn. 139), S. 88; HUANG Taiyun (Fn. 143), S. 15. Vgl. hierzu ein Urteil aus dem Jahr 2011, in dem das Oberstufengericht von Peking Mobiltelefonnummern als persönliche Daten im Sinne des § 253-1 Abs. 1 StGB identifizierte (谢新冲出售公民个人信息案: (2011) 高刑终字第招7号).

164 Vgl. *DIAO Shengxian/ZHANG Qiangqiang* (Fn. 141), S. 49.

bei dem Verkauf und der anderweitigen rechtswidrigen Weitergabe von persönlichen Daten, die von der jeweiligen Einheit im Zuge der Erfüllung ihrer Amtspflichten oder der Ausübung ihrer Dienstleistung erhoben wurden.[165] Allerdings sei bemerkt, dass auch der Diebstahl oder die anderweitige rechtswidrige Erlangung auch durch sonstige Personen von personenbezogenen Daten obiger Art[166] strafrechtlich sanktioniert wird,[167] wobei das Gesetz erneut den problematischen Ansatz der Sanktionierung nur „schwerwiegender Fälle" verwendet. Unklar bleibt, was unter „rechtswidriger Erlangung" konkret zu verstehen ist.[168] Grundsätzlich ist damit offenbar der widerrechtliche Kauf oder die Aneignung von personenbezogenen Daten insbesondere von den im vorangehenden Artikel erwähnten Einrichtungen und deren Mitarbeitern oder die Aneignung mittels Betrug oder Bestechung jeweils auch im Auftrag gemeint.[169]

Es fehlt zudem an einer konkreten Definition des Begriffs der persönlichen bzw. personenbezogenen Daten,[170] was laut DIAO/ZHANG insbesondere auf das Fehlen eines chinesischen Datenschutzgesetzes zurückzuführen ist, das eine solche Definition liefern könnte.[171] DIAO/ZHANG führen des weiteren den Mangel an, dass zwischen vorsätzlicher und fahrlässiger Handlung nicht unterschieden wird.[172] Zuletzt sei bemerkt, dass die Sanktionierung bereits des unerlaubten Zugriffs auf Daten problematisch ist, da grundsätzlich derjenige für den Schutz der Daten die Verantwortung tragen sollte, der diese unerlaubt zugänglich gemacht hat.

Für die Anwendung auf das Cloud-Computing ist insbesondere die Frage zu klären, inwiefern Cloud-Dienstleister unter den Regelungsbereich zu fassen sind. ZHANG Lei bemerkt, dass die jüngere Literatur zwar von einem breiten Interpretationsansatz ausgeht, das Gesetz grundsätzlich jedoch öffentlich-rechtliche Einrichtungen anspricht, die in einem staatlichen Auftrag agieren.[173] Ob Cloud-Dienstleister als im Gesetz benannte „Telekommunikationseinrichtungen" gelten können, bleibt daher von der zukünftigen Rechtsprechung zu klären. Grundsätzlich kann jedoch festgestellt werden, dass Unternehmen genannter Branchen bei der Nutzung von Cloud-Diensten ihrerseits unter den Regelungsbereich des § 253-1 StGB fallen.

Mit dem Schutz von personenbezogenen Daten über das StGB ist der Datenschutz nicht mehr nur im privatrechtlichen Umfeld zu finden. Trotz unklarer Voraussetzungen für eine Sanktionierung und einer eng gefassten Definition des Tatbestands kann zumindest von grundsätzlichen Strukturen zum Schutz personenbezogener Daten gesprochen werden. Unklar bleibt jedoch aufgrund einer fehlenden rechtlichen Definition, welche konkreten Daten als persönliche Daten im Sinne des StGB zu betrachten sind.

In der Literatur wird der Schutz personenbezogener Daten im StGB teilweise als grundsätzlich auf die Verletzung der Privatsphäre beschränkt verstanden,[174] so dass, folgt man dieser Betrachtung, das privatrechtlich kodifizierte Recht auf Privatsphäre in das Strafrecht hineinreicht. Teilweise wird in der Literatur jedoch auch der Begriff der persönlichen Daten von dem Begriff der Privatsphäre insoweit entkoppelt, als dass persönliche Daten auch – aber eben nicht ausschließlich – die Privatsphäre des Bürgers betreffende Daten umfassen können.[175] Eine rechtliche Definition ist an dieser Stelle also unbedingt wünschenswert.[176]

Zusammenfassend betrachtet kann auf der Grundlage der Regelungen zum Schutz von Privatsphäre und personenbezogenen Daten des DelHaftG und StGB jedenfalls nicht von einem umfassenden Datenschutz gesprochen werden, da es insbesondere an konkretisierten Regelungen zu den Rechten des Betroffenen auf Auskunft, Berichtigung, Sperrung oder Löschung fehlt. Angaben zum erlaubten Umfang der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten fehlen ebenso.

6.2 Der „Beschluss zur Stärkung des Datenschutzes"

Der „Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Stärkung des Datenschutzes in [elektronischen] Netzwerken" aus dem Jahre 2012 (StärkDatSchBeschl) ist eines der bisher umfassendsten Dokumente mit Gesetzesrang[177] im Bereich des Datenschutzes erlassen worden. Neben einer Definition des Rechtsgegenstandes führt

---

165 Vgl. § 253-1 Abs. 1 StGB.

166 Es ist nicht restlos geklärt, ob mit den in § 253-1 Abs. 2 StGB erwähnten „oben genannten Daten" generell „persönliche Daten" gemeint sind oder nur die nach § 253-1 Abs. 1 StGB durch die angeführten Einrichtungen erhobenen Daten. ZHANG Lei führt allerdings ein Urteil aus dem Jahr 2011 an, in dem auch Daten im Sinne des § 253-1 Abs. 2 StGB identifiziert wurden, die nicht über die in § 253-1 Abs. 1 StGB angeführten Einrichtungen erhoben wurden; vgl. *ZHANG Lei* (Fn. 140), S. 73.

167 Vgl. § 253-1 Abs. 2 StGB.

168 Vgl. *CHANG Qing/ZHANG Li* (Fn. 139), S. 88.

169 Vgl. *ZHANG Mingkai* (Fn. 144), S. 825.

170 Vgl. *CHANG Qing/ZHANG Li* (Fn. 139), S. 88.

171 Vgl. *DIAO Shengxian/ZHANG Qiangqiang* (Fn. 141), S. 49.

172 Vgl. *DIAO Shengxian/ZHANG Qiangqiang* (Fn. 141), S. 49.

173 Vgl. *ZHANG Lei* (Fn. 140), S. 74

174 Vgl. bspw. *ZHANG Mingkai* (Fn. 144), S. 824 f.

175 Vgl. bspw. *CHANG Qing/ZHANG Li* (Fn. 139), S. 88

176 Siehe ausführlich zum Begriffsdefinition der persönlichen Daten auch Punkt 9.2.

177 Diese Formulierung wurde hier gewählt, weil es sich bei dem Dokument nicht um eine administrative Verordnung handelt. Vielmehr ist es als eine ein Gesetz ergänzende Norm zu betrachten, auch wenn es selbst nicht die Qualität eines eigenständigen Gesetzes hat. Vgl. hierzu *Frank Münzel (Hrsg.), Knut B. Pißler,* Chinas Recht, 15.03.2000, 2 (Gesetzgebungsgesetz der VR China), Hamburg 2013, <http://www.chinas-recht.de/000315b.htm> eingesehen am 25. Oktober 2013, Fn. 3.

die Norm das Prinzip der Zustimmung durch den Betroffenen vor Erhebung und Nutzung seiner Daten sowie das Prinzip der Notwendigkeit an, das besagt, dass nur solche Daten erhoben werden dürfen, die für die Erreichung des mit dem Betroffenen vereinbarten Ziels notwendig sind. Sie greift dabei die bereits in der IntDienstlMarktR desselben Jahres formulierte Definition von persönlichen Daten auf.[178]

Zunächst findet sich in § 1 Abs. 1 StärkDatSchBeschl eine verklausulierte Definition des Begriffes der „persönlichen Daten", wenn es heißt, dass „[d]er Staat […] elektronische Daten [schützt], die geeignet sind, Rückschlüsse auf die persönliche Identität von Bürgern zu ziehen, und die die persönliche Privatsphäre von Bürgern betreffen"[179]. Es wird nicht ausdrücklich gesagt, dass mit dem im Folgenden verwandten Begriff der „elektronischen persönlichen Daten" eben diese vom Staat geschützten Daten gemeint sind, trotzdem kann § 1 Abs. 1 StärkDatSchBeschl wohl als allgemeingültige Definition für persönliche Daten herangezogen werden, da es bisher auf gesetzesrechtlicher Ebene an einer solchen gefehlt hat.[180] In § 1 Abs. 2 StärkDatSchBeschl heißt es ferner, dass „[k]eine Organisation und Einzelperson […] elektronische persönliche Daten von Bürgern[181] stehlen, sich rechtswidrig aneignen, verkaufen oder rechtswidrig […] an Dritte weitergeben [darf]"[182]. Eine Eingrenzung auf Daten, die im Zuge der behördlichen oder unternehmerischen Arbeit erhoben wurden, findet sich nicht, weswegen grundsätzlich sogar solche elektronischen Daten unter diese Regelungen fallen, die über Dritte oder auf nicht-elektronischem Wege erhoben wurden.[183] Es ist jedoch anzumerken, dass nicht eindeutig ist, ob mit dieser Formulierung auch persönliche Daten gemeint sind, die nicht direkt die Privatsphäre betreffen, wie beispielsweise Namen oder Telefonnummern. Im Gegensatz zur diesbezüglich eindeutigen Definition „persönlicher Daten" der IntDienstlMarktR ist hier außerdem unklar, ob auch solche Daten vom Regelungsbereich umfasst sind, die erst durch die Zusammenführung mit anderen Daten eine Identifikation des Datensubjekts ermöglichen.

Bei Erhebung und Nutzung von persönlichen Daten von Bürgern müssen Internetdienstanbieter und andere gewerbetreibende Unternehmen sowie vor allem deren Mitarbeiter die „Prinzipien der Legalität, der Rechtmäßigkeit und der Notwendigkeit befolgen, Ziel, Art und Rahmen der Erhebung und Nutzung der Daten darlegen sowie die Zustimmung des Betroffenen einholen"[184]. Die Regeln, die der Verarbeitung der persönlichen Daten zugrunde liegen, sind zudem bekannt zu machen.[185] Unklar ist hierbei, ob dem Betroffenen auch Informationen über die Weitergabe seiner Daten erteilt werden sollen. Den Informationspflichten des ISP stehen jedenfalls keine Rechte des Betroffenen auf Auskunft über die erhobenen Daten oder auf Berichtigung und Löschung der Daten gegenüber.

Die erhobenen Daten sind geheim zu halten,[186] und es sind „technische und andere nötige Maßnahmen zu ergreifen, die die Datensicherheit gewährleisten und die Preisgabe, Schädigung und den Verlust von elektronischen persönlichen Daten, die während der Geschäftsaktivität erhoben wurden, verhindern, [und] im Falle der erfolgten oder zu erwartenden Preisgabe, Schädigung oder des erfolgten oder zu erwartenden Verlustes sind unverzüglich Gegenmaßnahmen zu ergreifen"[187]. Was konkret unter den oben genannten „Prinzipien" zu verstehen ist,[188] welche konkreten Maßnahmen zum Datenschutz getroffen werden sollen und wie die so genannten „Gegenmaßnahmen" aussehen sollen, wird jedoch nicht näher ausgeführt.[189] Es folgen weitere Bestimmungen zu Nachrichten mit verbotenem Inhalt, deren Verbreitung bei Bekanntwerden zu verhindern, zu protokollieren und zu melden ist, ferner Regeln zum Versand kommerzieller Nachrichten sowie Regeln für ISP zur notwendigen Identifizierung ihrer Nutzer und Kunden. Mit letzterer Regelung wird ein Klarnamensystem rechtlich verankert, das die anonyme oder pseudonyme Nutzung von Internetdiensten unmöglich macht.[190]

---

178 S. hierzu ausführlich Punkt 7.2.

179 § 1 Abs. 1 „Beschluss des Ständigen Ausschusses des NVK zur Stärkung des Datenschutzes in [elektronischen] Netzwerken" (全国人大常务委员会关于加强网络信息保护的决定) vom 28. Dezember 2012 (StärkDatSchBeschl), Gazette of the Standing Committee of the National People's Congress of the People's Republic of China (中华人民共和国全国人民代表大会常务委员会公报), No. 1, Peking 2013, S. 62–63. Greenleaf bemerkt, dass die Regelungen damit auf chinesische Staatsbürger beschränkt sind; vgl. *Graham Greenleaf*, China's NPC Standing Committee Privacy Decision: A Small Step, Not a Great Leap Forward, in: Privacy Laws & Business International Report, Vol. 121, Pinner (Middlesex) 2013, <http://ssrn.com/abstract=2251303> eingesehen am 21. Juni 2013, S. 2.

180 Vgl. jedoch auf verwaltungsrechtlicher Ebene die entsprechende Definition in den „Richtlinien zur Regulierung der Marktordnung für Internetdienstleistungen" (规范互联网信息服务市场秩序若干规定) vom 7. Dezember 2011 (IntDienstlMarktR), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 17, Peking 2012, S. 29–31.

181 Chin.: 公民个人电子信息.

182 § 1 Abs. 2 StärkDatSchBeschl.

183 Vgl. *Tim Stratford* et al., E-Alert – Global Privacy & Data Security: China Enacts New Data Privacy Legislation, Beijing 2013, <http://www.cov.com/files/Publication/83ff413a-af68-4675-850e-a0f54533d149/Presentation/PublicationAttachment/240e4b51-6450-4403-8cfe-b0cea77c8370/China_Enacts_New_Data_Privacy_Legislation.pdf> eingesehen am 24. Mai 2013, S. 1.

184 § 2 Abs. 1 StärkDatSchBeschl.

185 Vgl. § 2 Abs. 2 StärkDatSchBeschl.

186 Vgl. § 3 StärkDatSchBeschl.

187 § 4 StärkDatSchBeschl.

188 Beachte jedoch zu diesen und weiteren „grundlegenden Prinzipien" GB/Z 28828-2012 (*AQSIQ/SAC*, Fn. 255) sowie Punkt 8.

189 Vgl. *Tim Stratford* et al. (Fn. 164), S. 2.

190 Vgl. *Tim Stratford* et al. (Fn. 164), S. 2. Insofern stärkt die StärkDatSchBeschl auch durchaus die Kontrolle von Internetnutzern und ist nicht ausschließlich auf die Stärkung eines Datenschutzes ausgelegt; vgl. *Graham Greenleaf* (Fn. 161), S. 2.

Im Falle des Bekanntwerdens von Rechtsverletzungen durch den Betroffenen – hier werden die Preisgabe der persönlichen Identität oder der Privatsphäre ausdrücklich erwähnt –, ist dieser berechtigt, den zuständigen ISP um Löschung oder Sperrung der entsprechenden Informationen zu ersuchen.[191] Handlungen, die Straftaten darstellen, können von jeder Organisation oder Einzelperson bei den zuständigen Behörden angezeigt werden. Die ISP haben mit den untersuchenden Behörden zusammenzuarbeiten und sie technisch zu unterstützen.[192] Die Behörden dürfen die im Zuge ihrer Arbeit erlangten Daten ihrerseits nicht verfälschen oder beschädigen oder an Dritte weitergeben.[193] Die Behörden haben unter anderem die Möglichkeit, die betroffene Internetseite zu sperren oder die weitere Ausübung der Internetdienstleistung durch die verantwortliche Person zu verbieten.[194]

Im Vergleich mit den IntDienstlMarktR liegt der Regelungsschwerpunkt der StärkDatSchBeschl offenbar eher auf der Kodifizierung von Pflichten des ISP, ein gewisses Maß an Datensicherheit zu gewährleisten, sowie auf der rechtlichen Verankerung eines Klarnamensystems. Wegen der allgemein gehaltenen Definitionen ist die StärkDatSchBeschl in vollem Maße auch für Cloud-Dienstleister von Bedeutung. Als Norm mit Gesetzesrang ergänzt die StärkDatSchBeschl die Regeln des DelHaftG und StGB insbesondere um eine Definition von personenbezogenen Daten wie um die genannten Prinzipien bei der Erhebung und Verarbeitung von personenbezogenen Daten. Dennoch erwachsen dem Datensubjekt nur auf der Grundlage der genannten Gesetze entsprechende Ansprüche. Grundlegende Rechte des Betroffenen auf Auskunft, Korrektur oder Löschung seiner Daten sind weiterhin nicht gesetzlich verankert.

7. Entwicklungen des Datenschutzes in administrativen Regelungen

In der Entwicklung des chinesischen Rechtssystems werden oftmals Lücken in spezialrechtlichen Bereichen zunächst durch Verwaltungsrechtsbestimmungen gefüllt, bevor ein allgemein gültiges und oft auch einen größeren Regelungsrahmen umfassendes Gesetz erlassen wird. Auch und gerade im Bereich des Internetrechts ist eine solche Entwicklung zu beobachten, wenn eine ganze Reihe von oft rasch in Folge erlassenen Verordnungen das gerade in Bezug auf das sich schnell entwickelnde Medium des Internets noch vergleichsweise defizitäre Zivil- und Strafrecht zu ergänzen versuchen. Nachfolgend sollen die für den Bereich des Cloud-Computing relevanten Regelungen dieser Verordnungen für die Internet-Branche näher betrachtet werden. Auch auf regionaler Ebene finden sich Regelungen zu den betrachteten Themen, aufgrund ihrer Vielzahl kann an dieser Stelle jedoch nur beispielhaft auf einzelne regionale Regelungen eingegangen werden.

7.1 Administrative Vorschriften für den Internet-Sektor

Obwohl Regelungen mit Internetbezug bereits seit 1994 existieren,[195] lässt sich erst mit den „Fernmeldebestimmungen der VR China“ von 2000 (FernmBest), die grundsätzlich den Schutz von Rechten und Interessen Dritter auch im Internet festschreiben,[196] eine Grundlage für den expliziten Schutz von Privatsphäre und personenbezogenen Daten im Internetbereich finden.[197] In den FernmBest heißt es ferner, dass keine Organisation oder Einzelperson Informationen über das Internet verbreiten darf, die die Rechte und Interessen Dritter verletzen,[198] außerdem dürfen Informationen Dritter nicht zerstört werden.[199] Des weiteren wird der Schutz der Kommunikationsfreiheit und des Briefgeheimnisses explizit auch für Internetnutzer als gültig erklärt.[200] Im Anhang der FernmBest werden zudem in einer Übersicht verschiedene Telekommunikationsdienste in „Basis-“ und „Value-Added-Dienste“ unterteilt. Unter letzteren werden unter anderem „Internetzugangsdienstleistungen“[201] und „Internetinformationsdienstleistungen“[202] angeführt. Mit dieser Einordnung liefern die FernmBest die Grundlage für weitere Vorschriften und

---

191 Vgl. § 8 StärkDatSchBeschl.

192 Vgl. §§ 9 und 10 StärkDatSchBeschl.

193 Vgl. § 10 Abs. 2 StärkDatSchBeschl; vgl. auch die entsprechenden Regelungen des § 253-1 StGB.

194 Vgl. § 11 StärkDatSchBeschl.

195 Den Beginn einer ganzen Reihe von internetrechtlichen Bestimmungen machen die „Bestimmungen der VR China zum Schutz der Sicherheit von EDV-Systemen“ (计算机信息系统安全保护条例) von 1994.

196 In § 6 „Fernmeldebestimmungen der VR China“ (中华人民共和国电信条例) vom 25. September 2000 (FernmBest) heißt es, dass „keine Organisation oder Einzelperson […] vermittels des Internets Aktivitäten ausüben [darf], die die Staatssicherheit, die öffentlichen Interessen der Gesellschaft oder die legalen Rechte und Interessen Dritter gefährden“. Die FernmBest finden sich in Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 33, Peking 2000, S. 11–21.

197 In § 18 „Durchführungsbestimmungen zu den vorläufigen Richtlinien der VR China zur Verwaltung internationaler EDV-Systeme“ (中华人民共和国计算机信息网络国际联网管理暂行规定实施办法) vom 13. Februar 1998 (abgedruckt in New Laws and Regulations Monthly (新法规月刊]) No. 7, Shanghai 1998, S. 28–30) findet sich zwar bereits der Begriff der Privatsphäre, jedoch nur insofern, als der Internetnutzer bei der Veröffentlichung von Informationen im Internet die Privatsphäre Dritter zu beachten hat. Konkrete Regelungen für Anbieter von Dienstleistungen im Internet fehlen. Laut § 22 werden dem § 18 zuwiderlaufende Handlungen nach dem Gesetz bestraft, spezielle Rechtsfolgen werden jedoch nicht genannt.

198 Vgl. § 57 Abs. 8 FernmBest.

199 Vgl. § 58 FernmBest.

200 Vgl. § 66 FernmBest.

201 Chin.: 互联网接入服务.

202 Chin.: 互联网信息服务.

rechtliche Regelungen, die sich in konkreter Form an Anbieter von Internet-Dienstleistungen richten.

7.2 Spezielle Vorschriften für Anbieter von Internet-Dienstleistungen

Ab 2000 wurden ergänzend zu den allgemeinen Vorschriften für die elektronische Datenverarbeitung in Netzwerken konkrete Regelungen für Dienstleister im Internet eingeführt. Die „Maßnahmen zu Internetdienstleistungen" von 2000 (IntDienstlM) definieren eine Unterteilung von ISP in kommerzielle und nicht-kommerzielle Anbieter.[203] Die „Richtlinien zur Administration von elektronischen Nachrichtendienstleistungen im Internet" aus demselben Jahr (IntNachrDienstlR) enthalten erstmalig das Prinzip der Zustimmung des Betroffenen. Ohne eine solche Zustimmung dürfen keine Daten des Betroffenen an Dritte veröffentlicht werden.[204] Im Falle der unerlaubten Veröffentlichung ist es die Aufgabe der lokalen Telekommunikationsbehörden, für Abhilfe zu sorgen; ist dem Betroffenen ein Schaden entstanden, ist die zivile Haftung nach dem Gesetz zu übernehmen.[205]

Die „Richtlinien zur Regulierung der Marktordnung für Internetdienstleistungen" von 2012 (IntDienstlMarktR) gelten für alle „Internetinformation sdienstleistungen"[206] sowie mit solchen Diensten in Bezug stehende Aktivitäten.[207] Greenleaf (2012) sieht aufgrund des begrifflichen Rückbezugs auf die IntDienstlM von 2000 nicht nur Internetdienstanbieter von der Regelung umfasst, sondern allgemein jeden, der im Internet Informationen anbietet, jedenfalls sowohl kommerzielle als auch nicht-kommerzielle Anbieter, nicht jedoch den öffentlichen Sektor.[208] Besonders hervorzuheben ist das in diesem Regelwerk erstmalig formulierte Prinzip der Notwendigkeit: Außer Daten, die für die Ausübung der vorher mit dem Betroffenen durch dessen ausdrückliche Zustimmung vereinbarten Dienstleistung notwendig sind, dürfen vom ISP keine Daten erhoben werden. Die erhobenen Daten dürfen nur für die vereinbarte Dienstleistung verwendet werden.[209] Zudem muss der Betroffene der Erhebung seiner Daten zustimmen und vom ISP über die Art und Weise der Erhebung und Verarbeitung seiner Daten und deren Inhalt informiert werden.[210] Greenleaf bemerkt allerdings, dass eine solche Informationspflicht jedenfalls für den ISP offenbar nicht gilt, wenn die Daten über Dritte erhoben werden.[211]

ISP dürfen ohne die Zustimmung des Nutzers[212] keine Daten, die der Nutzer hochgeladen hat, weitergeben.[213] Allerdings ist unklar, ob der ISP Daten, die er selbst über den Nutzer generiert hat oder von Dritten erhalten hat, weitergeben darf oder nicht.[214] Der ISP hat zudem für die Sicherheit und Konsistenz (nicht aber über die Qualität und Aktualität) der Daten des Nutzers „Sorge zu tragen"[215]; der Nutzer soll die Kontrolle über seine Daten behalten.[216] Die Richtlinien erkennen erstmalig an, dass durch die Zusammenführung von an sich nicht zuordenbaren personenbezogenen Daten mit anderen Daten unter Umständen eine Zuordenbarkeit entstehen kann,[217] und bieten damit überhaupt erstmalig im chinesischen Recht eine Definition für persönliche Daten.[218] Die grundlegenden Rechte des Datensubjekts, über die erhobenen personenbezogenen Daten Auskunft einholen und sie korrigieren, sperren oder löschen zu können, fehlen im vorliegenden Regularium.[219]

Als Aufsichtsbehörden fungieren das Ministerium für Industrie und Informationstechnik (MIIT)[220] und untergeordnete Telekommunikationsbehörden.[221] Die Vollstreckung der Regeln wird durch diese Behörden initiiert, die für Verstöße gegen die Vorschriften bezüglich persönlicher Daten des Nutzers Bußgelder zwischen 10.000 und 30.000 RMB erheben können.[222] Wenn Daten illegalerwei-

---

203 Vgl. § 3 „Maßnahmen zu Internetdienstleistungen" (互联网信息服务管理办法) vom 25. September 2000 (IntDienstlM), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 34, Peking 2000, S. 7–9.

204 Vgl. § 12 „Richtlinien zur Administration von elektronischen Nachrichtendienstleistungen im Internet" (互联网电子公告服务管理规定) vom 8. Oktober 2000 (IntNachrDienstlR), Gazette of the State Council of the People's Republic of China (中华人民共和国国务院公报), No. 25, Peking 2001, S. 42–43; *HONG Hailin* (Fn. 4), S. 156.

205 Vgl. § 19 IntNachrDienstlR.

206 Chin: 互联网信息服务.

207 Vgl. § 2 IntDienstlMarktR.

208 Vgl. *Graham Greenleaf,* China's Internet Data Privacy Regulations 2012: 80 % of a Great Leap Forward?, in: Privacy Laws & Business International Report, Vol. 116, Pinner (Middlesex) 2012, <http://ssrn.com/abstract=2049232> eingesehen am 30. Mai 2013, S. 4 f. Jedoch sehen Stratford/Carlson/Livingston aufgrund des inhaltlichen Kontextes der Richtlinie jedenfalls Anbieter von Drahtlos-Breitbandnetzwerken im Mobilfunkbereich nicht von der Regelung umfasst; vgl. *Tim Stratford/Eric Carlson/Scott Livingston,* E-Alert: China Practice – New Internet Competition Rules in China Include Personal Data Protections, Beijing 2012, <http://www.cov.com/files/Publication/28481074-55b3-45fc-b666-f6c818d8b8b8/Presentation/PublicationAttachment/1d6b6639-e0a1-43d2-891d-024aca8600a6/New%20Internet%20Competition%20Rules%20in%20China%20Include%20Personal%20Data%20Protections.pdf> eingesehen am 1. Juni 2013, S. 1.

209 Vgl. § 11 IntDienstlMarktR; *Graham Greenleaf* (Fn. 186), S. 3.

210 Vgl. § 11 IntDienstlMarktR.

211 Vgl. *Graham Greenleaf* (Fn. 186), S. 3.

212 Chin.: 用户.

213 Vgl. § 13 IntDienstlMarktR.

214 Vgl. *Graham Greenleaf* (Fn. 186), S. 4. Stratford/Carlson/Livingston geben sogar zu Bedenken, dass nicht mit Sicherheit gesagt werden kann, dass mit den „hochgeladenen Daten" auch personenbezogene Daten gemeint sind; vgl. *Tim Stratford/Eric Carlson/Scott Livingston* (Fn. 186), S. 2.

215 Chin.: 妥善保管.

216 Vgl. §§ 12, 13 IntDienstlMarktR; *Graham Greenleaf* (Fn. 186), S. 4.

217 Vgl. § 11 IntDienstlMarktR.

218 Die Richtlinie beschränkt sich allerdings auf „persönliche Daten des Nutzers"; vgl. dazu auch Punkt 9.2. Vgl. *Tim Stratford/Eric Carlson/Scott Livingston* (Fn. 186), S. 1 f.

219 Vgl. *Graham Greenleaf* (Fn. 186), S. 4 f.

220 Chin.: 中华人民共和国工业和信息化部. Das Ministerium für Informationsindustrie (信息产业部) ist 2008 im MIIT aufgegangen.

221 Vgl. § 3 IntDienstMarktRegR; *Graham Greenleaf* (Fn. 186), S. 3.

222 Vgl. §§ 16, 18 IntDienstlMarktR; *Graham Greenleaf* (Fn. 186), S. 5.

se publik werden, sind die Aufsichtsbehörden, in schweren Fällen das MIIT, direkt zu informieren. Es wird nicht definiert, was unter „schweren Fällen" zu verstehen ist.[223] Obgleich eine Information an die betroffenen Nutzer nicht explizit erwähnt wird, ist nach Greenleaf eine Aufforderung des MIIT an die ISP zur Benachrichtigung der Betroffenen üblich.[224]

Die Regelungen der IntDienstlMarktR können grundsätzlich auf Anbieter von Cloud-Diensten angewendet werden. Für die Nutzung von Cloud-Diensten ist insbesondere das Verbot der Weitergabe von durch den Nutzer hochgeladenen Daten ohne seine Zustimmung von hoher Relevanz. Allerdings ist fraglich, ob die Zustimmung des Nutzers auch dann erforderlich ist, wenn eine zwischengeschaltete Stelle, die nicht selbst als ISP einzuordnen ist, dessen Daten an den Cloud-Dienstleister weitergibt. Auch scheint in einem solchen Falle die Informationspflicht des ISP zumindest nicht gegenüber dem Datensubjekt zu bestehen.

Die „Richtlinien für den Schutz persönlicher Daten in der Telekommunikation und im Internet" vom 28. Juni 2013 (TelIntDatSchR) präzisieren den Begriff der personenbezogenen Daten durch Angabe von konkreten Beispielen[225] und geben detailliertere Vorgaben, was das Informieren des Nutzers über Umfang und Verwendung der erhobenen Daten,[226] über dessen Möglichkeiten, seine Daten abzurufen und zu ändern, sowie über die getroffenen Regelungen des Unternehmens zum Umgang mit personenbezogenen Daten. Auch müssen Unternehmen nach Beendigung der Nutzung des betreffenden Dienstleistung durch den Nutzer die Erhebung und Nutzung[227] seiner Daten beenden sowie ihm eine Möglichkeit zur Löschung seines Kontos bzw. seiner Nummer geben.[228]

Insbesondere für den Bereich des Cloud-Computing relevant sind die neuen Regelungen zur Verarbeitung von Daten durch Dritte. Personenbezogene Daten dürfen nur an solche Dritte zur Verarbeitung weitergegeben werden, die den Anforderungen der Bestimmung genügen.[229] Neu ist auch das Erfordernis, ein internes Sicherheitsmanagement mit konkret definierten Arbeitsabläufen und einer kontrollierten Rechtezuweisung einzurichten und damit den Zugriff auf personenbezogene Daten auch innerhalb des Unternehmens zu beschränken. Die Daten sind zudem gegen unerlaubte Zugriffe zu sichern und jede Verarbeitung der Daten ist zu dokumentieren.[230] Die o.g. Vorschriften können durch das MIIT und untergeordneten Telekommunikationsbehörden mit einer Verwarnung oder Geldbuße von 10.000 bis 30.000 RMB geahndet werden.[231]

Zusammenfassend lässt sich festhalten, dass die TelIntDatSchR einige der Mängel der vorangegangenen IntDienstlMarktR beheben, insbesondere das Recht des Nutzers auf Einsicht und Änderung seiner Daten. Mit der Beendigung der Nutzung einer Dienstleistung dürfen zumindest keine weiteren Daten erhoben werden und die Nutzung von erhobenen Daten muss unterbleiben. Ob allerdings die Löschung des Kontos oder der Nummer gleichbedeutend mit der Löschung aller relevanten personenbezogenen Daten ist, ist nicht ganz eindeutig. Problematisch bleibt die Eingrenzung auf personenbezogene Daten des Nutzers[232], womit offen bleibt, wie mit personenbezogenen Daten Dritter zu verfahren ist.

7.3 Ausgewählte regionale Verwaltungsrechtsbestimmungen

Auch auf regionaler Ebene sind vereinzelt Bestimmungen erlassen worden, deren Ziel ein stärkerer Schutz von personenbezogenen Daten ist. Aufgrund der Vielzahl der regionalen Bestimmungen sollen an dieser Stelle lediglich zwei beispielhaft herausgegriffen werden.

Dies sind zum einen die 2003 von der Stadtregierung Shanghai erlassenen „Maßnahmen zur Erhebung von personenbezogenen Kreditinformationen (zur testweisen Durchführung)", deren klarer schematischer Aufbau Grundzüge eines Datenschutzgesetzes aufweist, weswegen hier trotz der eingeschränkten Anwendung der Regelungen auf Kreditinformationen eine kurze Betrachtung erfolgen soll.[233] Im ersten Abschnitt findet sich zunächst eine Definition des in den Bestimmungen verwen-

---

223 Vgl. *Tim Stratford/Eric Carlson/Scott Livingston* (Fn. 186), S. 2.

224 Greenleaf führt als Beispiel einen entsprechenden Fall aus dem Jahre 2011 an; vgl. *Graham Greenleaf* (Fn. 186), S. 4.

225 Zu personenbezogenen Daten zählen danach neben Name, Geburtsdatum, Personalausweisnummer, Adresse, Telefonnummer sowie den Zugangsdaten zur Dienstleistung auch der Zeitpunkt und der Ort des Zugriffs durch den Nutzer; vgl. § 4 „Richtlinien für den Schutz persönlicher Daten in der Telekommunikation und im Internet" (电信和互联网用户个人信息保护规定) vom 28. Juni 2013 (TelIntDatSchR), chinesischer Text online einsehbar unter <www.pkulaw.cn/fulltext_form.aspx?Db=chl&Gid=207021&keyword=电信和互联网用户个人信息保护规定&EncodingName=&Search_Mode=accurate> (zuletzt eingesehen am 12. Dezember 2013).

226 Vgl. § 9 TelIntDatSchR; vgl. auch *Daniel Cooper* et al.: E-Alert: Privacy & Data Security – China Issues Comprehensive Regulation on Collection and Use of Personal Information by Internet and Telecommunication Service Providers, Beijing 2013, <http://www.cov.com/files/Publication/3024dd1a-ab7e-4437-805d-139dbb96a713/Presentation/PublicationAttachment/527b0441-8c91-4e08-a866-175d89b796a9/China_Issues_Comprehensive_Regulation_on_Collection_and_Use_of_Personal_Information_by_Service_Providers.pdf> eingesehen am 25. Oktober 2013, S. 1.

227 Chin.: 使用.

228 Vgl. § 9 TelIntDatSchR; vgl. *Daniel Cooper* (Fn. 203), S. 1.

229 Vgl. § 11 TelIntDatSchR; vgl. *Daniel Cooper* (Fn. 203), S. 2.

230 Vgl. § 13 TelIntDatSchR; vgl. *Daniel Cooper* (Fn. 203), S. 2.

231 Vgl. § 23 TelIntDatSchR; vgl. *Daniel Cooper* (Fn. 203), S. 3.

232 Chin.: 用户.

233 So sieht es bspw. JIANG, wenn Sie von einem „Prototyp eines Datenschutzgesetzes" spricht. Vgl. *JIANG Ge* (Fn. 142), S. 645.

deten Begriffs der „personenbezogenen Kreditinformationen" sowie eine Nennung der zuständigen Behörden. Es folgen abschnittsweise Regelungen zur Erhebung der Informationen, zur Verarbeitung der Informationen, zur Bereitstellung bzw. Weitergabe der Informationen, zum Widerspruch durch Datensubjekte sowie Regelungen zu Aufsicht und Kontrolle und zur rechtlichen Haftung.[234]

Bemerkenswert ist dabei die Detailliertheit der Regelungen. So wird im zweiten Abschnitt zur Erhebung der Informationen das Zustimmungsprinzip (mit konkretisierten Ausnahmen) definiert[235] und der Inhalt der zu erhebenden Informationen geregelt, auch dahingehend, welche Inhalte nicht erhoben werden dürfen.[236] Im Abschnitt zur Verarbeitung heißt es zusätzlich, dass die erhobenen Informationen sofort und unverändert abgespeichert werden müssen. Informationen, die nicht erhoben werden dürfen, dürfen auch nicht abgespeichert werden.[237]

Der Abschnitt zur Bereitstellung bzw. Weitergabe verneint grundsätzlich die Weitergabe von Informationen ohne die Zustimmung des Betroffenen[238] und definiert klare Ausnahmen von dieser Regel. Der Betroffene hat ein Auskunftsrecht über seine Daten, deren Herkunft und deren Abfrage durch Dritte.[239] Im Abschnitt zum Widerspruch des Datensubjektes wird außerdem das Recht des Betroffenen auf Berichtigung seiner Daten definiert.[240] Die Aufsicht obliegt Kreditprüfungsorganisationen, die schwere Fälle der städtischen Regulierungsbehörde melden müssen.[241] Regelwidriges Verhalten kann bei der städtischen Regulierungsbehörde angezeigt werden.[242] Abgesehen von der alleinigen Anwendbarkeit auf Kreditinformationen und geografisch auf die Provinzebene enthalten die oben genannten Maßnahmen Regelungen für einen umfassenden Datenschutz angefangen von klaren Definitionen des Rechtsobjektes bis hin zu den Rechten des Datensubjekts und der rechtlichen Durchsetzung. Offenbar stellt jedoch ein solch detailliertes Regelwerk jedenfalls für den Bereich des Datenschutzes eine Ausnahme dar.

Als zweite regionale Bestimmung sollen die 2013 in Kraft getretenen „Maßnahmen der Stadt Xiamen zum Schutz von persönlichen Daten im Software- und Informationsdienstleistungssektor" als Beispiel für ein aktuelles regionales Regelwerk zum Datenschutz betrachtet werden. Als Definition des verwendeten Begriffes der „persönlichen Daten" nennen die Maßnahmen „Informationen, die einer konkreten natürlichen Person zugeordnet sind und die einzeln oder in Kombination mit anderen Daten geeignet sind, durch rationales Überlegen oder Verarbeiten diese zugeordnete konkrete natürliche Person zu identifizieren, einschließlich Informationen zum Namen, Geburtstag, Ausweisnummer, Kontaktanschrift, Telefonnummer, Familienstand, Anstellungsverhältnis [sowie] Einkommenssituation […]"[243]. Als „Verarbeiten"[244] im Sinne der Bestimmungen wird das „Erheben, Bearbeiten[245], Weitergeben, Nutzen, Sperren [und] Löschen"[246] der Daten verstanden.

Als Aufsichtsinstanzen werden die städtischen Informationsbehörden genannt, die auch die jeweiligen Branchenverbände mit bestimmten Aufgaben betrauen können. Für Betriebe der Software- und Informationsindustrie, die persönliche Daten verarbeiten, wird bei den Informationsbehörden eine Akte hinterlegt. Die Verarbeitung von persönlichen Daten muss „einem festgelegten, klaren und vernünftigen Ziel und Rahmen [folgen]" und es muss „zuerst das Einverständnis des Datensubjekts eingeholt"[247] werden. Es müssen ein System für den Schutz von persönlichen Daten und ein „Notfallplan"[248] eingerichtet sowie Personal für die Aufsicht über die Datensicherheit zugeordnet werden.[249] Bei der Verarbeitung der Daten ist die Preisgabe, der Verlust, die Zerstörung, die Verfälschung und die unbefugte Verwendung der Daten zu verhindern.[250]

Das Datensubjekt, definiert als die den persönlichen Daten zugeordnete natürliche Person, hat ein Auskunftsrecht sowie ein Recht auf Berichtigung.[251] Eine unerlaubte Verwendung seiner Daten durch die Betriebe kann der Betroffene bei den zuständigen Behörden anzeigen, die den Fall dann verifizieren und bearbeiten.[252] Die angeführten Verwaltungsstrafen beziehen sich lediglich auf das Vor-

---

234 Vgl. *JIANG Ge* (Fn. 142), S. 645.

235 Vgl. § 7 „Maßnahmen der Stadt Shanghai zur Erhebung von personenbezogenen Kreditinformationen (zur testweisen Durchführung)" (上海市个人信用征信管理试行办法) vom 28. Dezember 2003 (SH-KredInfoM), New Laws and Regulations Monthly (新法规月刊), No. 2, Shanghai 2004, S. 32–36.

236 Vgl. § 8 SH-KredInfoM.

237 Vgl. § 10 SH-KredInfoM.

238 Vgl. §§ 14, 15 SH-KredInfoM.

239 Vgl. § 18 SH-KredInfoM.

240 Vgl. §§ 20–23 SH-KredInfoM.

241 Vgl. § 27 SH-KredInfoM.

242 Vgl. § 28 SH-KredInfoM.

243 § 3 Abs. 1 „Maßnahmen der Stadt Xiamen zum Schutz von persönlichen Daten im Software- und Informationsdienstleistungssektor" (厦门市软件和信息服务业个人信息保护管理办法) vom 19. November 2012 (XM-InfDienstlDatSchM), chinesischer Text online einsehbar unter <http://www.fzj.xm.gov.cn/html/2012-12/20121211163622.htm> (zuletzt eingesehen am 12. Dezember 2013).

244 Chin.: 处理.

245 Chin.: 加工.

246 § 3 Abs. 2 XM-InfDienstlDatSchM.

247 § 11 Abs. 1 XM-InfDienstlDatSchM.

248 Chin.: 应急处置预案,

249 Vgl. § 11 Abs. 2 XM-InfDienstlDatSchM.

250 Vgl. § 11 Abs. 3 XM-InfDienstlDatSchM.

251 Vgl. § 13 XM-InfDienstlDatSchM.

252 Vgl. § 14 XM-InfDienstlDatSchM.

handensein einer Akte. Verstöße gegen den Datenschutz werden nicht ausdrücklich sanktioniert.[253]

Im Gegensatz zu den Shanghaier Maßnahmen zu Kreditinformationen präsentieren sich die Maßnahmen zum Datenschutz aus Xiamen weniger detailliert und bieten dem Betroffenen grundsätzlich weniger Schutz. Positiv zu bewerten ist jedenfalls eine konkrete Definition des Rechtsobjektes, die auch Beispiele zur Verdeutlichung anführt, sowie die ausführliche Definition des „Verwendens" von persönlichen Daten. Weniger positiv zu bewerten ist allerdings die schwache Möglichkeit der Rechtsdurchsetzung für den Betroffenen und das Fehlen von Regelungen sowohl für interne als auch für unabhängige externe Kontrollmechanismen und -instanzen. Auf den Bereich des Cloud-Computing bezogen sind klar strukturierte und definierte Regelungen, wie sie die SH-KredInfoM bieten, wünschenswert. Insbesondere hervorzuheben sind hier die vergleichsweise strengen Regelungen der SH-KredInfoM zur Weitergabe der Daten an Dritte sowie deren Definition von Aufsichts- und Kontrollorganen und deren Aufgaben.

Obwohl nur regional verankerte Regelungen zum Datenschutz keine ausreichende Grundlage für den Schutz personenbezogener Daten bieten können, haben doch die angeführten Beispiele möglicherweise einen Vorbildcharakter für in Zukunft zu erlassene überregionale Normen.

8. Normen zur Standardisierung von Maßnahmen zum Datenschutz

Neben der Vielzahl an administrativen Regelungen sind in jüngerer Zeit auch Standardisierungsmaßnahmen zum Datenschutz getroffen worden. Erwähnenswert sind die „Richtlinien für den Schutz persönlicher Daten in öffentlichen und kommerziellen Informationssystemen (GB/Z 28828-2012)", die am 5. November 2012 verkündet worden und am 1. Februar 2013 in Kraft getreten sind. Sie greifen zum großen Teil Begriffsdefinitionen und Prinzipien für den Umgang mit persönlichen Daten aus bereits erlassenen Regelungen auf. Die Norm ist eine unverbindliche Norm, was sie grundsätzlich nicht als rechtliche Grundlage zur Durchsetzung von Rechten qualifiziert.[254] Wenn in der Norm in Punkt 4.1.2 das Recht des Betroffenen herausgestellt wird, in bestimmten Fällen gegen die datenverarbeitende Stelle zu klagen,[255] so ist dies daher lediglich als Verweis auf entsprechende Gesetze zu verstehen. Hervorzuheben ist jedoch trotz der fehlenden rechtlichen Verbindlichkeit der Versuch, in dieser Norm für den Datenschutz relevante Begriffe klar zu definieren, Akteure und deren Pflichten und Aufgaben festzulegen, den Prozess der Datenverarbeitung in klar umrissene Schritte zu gliedern sowie Grundprinzipien der Datenverarbeitung aufzustellen.[256] Die Definitionen in dieser Norm können des weiteren möglicherweise als definitorische Grundlage in Gerichtsurteilen hinzugezogen werden.[257]

Persönliche Daten werden im Sinne der Norm als „in Informationssystemen verarbeitbare und auf bestimmte Personen bezogene EDV-Daten" definiert, „die geeignet sind, allein oder durch Zusammenführung mit anderen Daten diese bestimmte Person zu identifizieren"[258]. Die Norm unterteilt gewöhnliche und sensible persönliche Daten. Letztere sind solche, die bei Preisgabe oder Veränderung dem Datensubjekt schaden. Als Beispiele werden Personalausweisnummer, Mobiltelefonnummer, ethnische Zugehörigkeit, politische Ansichten, religiöse Überzeugung, genetische und biometrische Daten genannt.[259] Die Norm kennt des weiteren eine Unterscheidung zwischen stillschweigender und ausdrücklicher Zustimmung, wobei von stillschweigender Zustimmung auszugehen ist, wenn kein ausdrücklicher Widerspruch des Betroffenen vorliegt.[260] Bei der Erhebung sensibler Daten oder persönlicher Daten von Minderjährigen sowie bei der Weitergabe oder dem Export von persönlichen Daten ist grundsätzlich eine ausdrückliche Zustimmung des Betroffenen erforderlich.[261] Allerdings wird in der Norm nicht definiert, auf welche Art diese ausdrückliche Zustimmung vollzogen werden soll.[262]

---

[253] Vgl. § 16 XM-InfDienstlDatSchM.

[254] §§ 14 und 20 StandardG sehen eine Implementierungspflicht bzw. rechtliche Haftung nur für verbindliche Normen (强制性标准) vor. Vgl. Fn. 15 zur Unterscheidung verschiedener Arten von Normen.

[255] S. *General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China (AQSIQ)/Standardization Administration of the People's Republic of China (SAC)* (中华人民共和国国家质量监督检验检疫总局/中国国家标准化管理委员会), GB/Z 28828-2012: Information Security Technology—Guideline for Personal Information Protection within Information System for Public and Commercial Services (信息安全技术——公共及商用服务信息系统个人信息保护指南), ohne Ortsangabe [Beijing] 2012, S. 2 (Punkt 4.1.2).

[256] Vgl. *China Software Testing Center (CSTC)* (中国软件评测中心) et al., Personal Information Protection in Information System and Standardization (信息系统个人信息保护与标准化), in: Information Technology & Standardization (信息技术与标准化), Vol. 1–2, Beijing 2012, S. 19 f.

[257] Vgl. *Daniel Cooper/Eric Carlson/Scott Livingston,* E-Alert – Global Privacy & Data Security: China Releases New National Standard for Personal Information Collected Over Information Systems, Beijing 2013, <http://www.cov.com/files/Publication/a180859b-c1ab-4ecf-a274-e6d-1a7b5fb2e/Presentation/PublicationAttachment/c8aad899-85f3-4d26-bb06-f0518ee09e20/China_Releases%20_New_National_Standard_for_Personal_Information_Collected_Over_Information_Systems.pdf> eingesehen am 24. Mai 2013, S. 1.

[258] *AQSIQ/SAC* (Fn. 226), S. 1 (Punkt 3.2).

[259] Vgl. *AQSIQ/SAC* (Fn. 226), S. 2 (Punkt 3.7).

[260] Vgl. *AQSIQ/SAC* (Fn. 226), S. 2 (Punkt 3.10, 3.11); *Graham Greenleaf/George Yijun Tian,* China Expands Data Protection through 2013 Guidelines: A "Third Line' for Personal Information Protection, with a Translation of the Guidelines, in: Privacy Laws & Business International Report, Vol. 122, Pinner (Middlesex) 2013, <http://ssrn.com/abstract=2280037> eingesehen am 21. Juni 2013, S. 4.

[261] Vgl. *AQSIQ/SAC* (Fn. 226), S. 4 f. (Punkt 5.3.4, 5.4.5); *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 4.

[262] Vgl. *Daniel Cooper/Eric Carlson/Scott Livingston* (Fn. 228) S. 3.

Die Norm definiert zudem verschiedene Akteure. Neben dem Datensubjekt selbst definiert sie einen „Beauftragten für persönliche Daten“ [263], womit eine Institution gemeint ist, die über Art und Ziel der Verarbeitung entscheidet,[264] für die Umsetzung der datenschutzrechtlichen Regeln im Betrieb zuständig ist, das Datensubjekt über unerwünschte Veröffentlichung, Löschung oder Veränderung seiner Daten informiert und schwerwiegende Fälle den zuständigen Behörden meldet.[265] Des weiteren versteht die Norm unter einem „Empfänger persönlicher Daten“ [266] Einzelpersonen oder Organisationen, die Daten „aufgrund des Willens des Datensubjekts verarbeiten“ [267] und nach Vollendung des Verarbeitungsprozesses löschen.[268] Diese Definition entspricht offenbar einer verarbeitenden Stelle, die personenbezogene Daten nur aufgrund der Zustimmung des Betroffenen verarbeiten darf.[269] Schließlich definiert die Norm eine „unabhängige Prüforganisation“ [270], die für die neutrale Kontrolle und Überwachung der Informationsverarbeitungsprozesse zuständig ist.[271]

Die Norm hebt grundlegende Prinzipien der Datenverarbeitung hervor, die die mit der Datenverarbeitung beauftragte Stelle bei der Verarbeitung von persönlichen Daten zu befolgen hat.[272] Danach muss das Ziel der Verarbeitung klar festgelegt und rational nachvollziehbar sein; es dürfen nur solche Daten erhoben werden, die zur Erfüllung des Ziels notwendig sind, und nach Erreichung des Ziels sind die Daten zu löschen.[273] Dem Betroffenen sind das Ziel der Erhebung, Nutzung und Umfang der Daten und Dauer der Speicherung sowie ergriffene Schutzmaßnahmen und Art und Umfang der eventuellen Weitergabe an Dritte auf Verlangen verständlich zu erläutern.[274] Ohne die – je nach Datentyp ausdrückliche oder stillschweigende – Einwilligung des Betroffenen dürfen keine Daten erhoben werden.[275] Während der Verarbeitung sind die Daten vertraulich, vollständig, verlässlich und aktuell zu halten; es sind geeignete Schutzmechanismen zu ergreifen, die insbesondere ein unkontrolliertes Auffinden oder Preisgeben sowie Verlust, Zerstörung und Verfälschung der Daten verhindern.[276] Die verarbeitende Stelle hat sich an Vertrag und Gesetz zu halten, nach Erreichung des vereinbarten Ziels ist die weitere Erhebung zu unterlassen.[277] Es sind klare Verantwortlichkeiten zu etablieren sowie der Verarbeitungsprozess zu protokollieren, Name und Anschrift des Verantwortlichen – im Falle der Weitergabe an eine andere Stelle auch des Verantwortlichen der anderen Stelle – sind dem Betroffenen mitzuteilen.[278]

Obgleich ohne verbindlichen Charakter weist die genannte Norm eine hohe Detailliertheit auf. Hervorzuheben ist die Forderung nach klaren Verantwortlichkeiten innerhalb der verarbeitenden Stelle sowie einer Protokollierung der Datenverarbeitung, was eine interne Aufsicht und Kontrolle ermöglicht. Zwar stellen Greenleaf/Tian fest, dass die Norm implizit Rechte des Betroffenen auf Auskunft und Korrektur[279] sowie auf Löschung der Daten[280] definiert,[281] aufgrund ihrer fehlenden Qualifikation als Rechtsnorm entwickelt sie daraus jedoch keinerlei Rechtsansprüche des Betroffenen. Hervorzuheben ist ferner die genaue Beschreibung der Norm über die Informationen, die dem Betroffenen mitzuteilen sind, einschließlich Informationen zu Weiterleitung und Verantwortlichkeiten. Bisherigen Regelungen fehlte es an einer solchen Präzision.[282] Eine besonders für die grenzüberschreitende Nutzung des Cloud-Computing relevante Regelung besteht im grundsätzlichen Verbot des Datenexports ins Ausland ohne die ausdrückliche Zustimmung des Datensubjekts, das auch für Datentransfers innerhalb eines Unternehmens gilt.

Aufgrund ihres offiziellen Status als vom MIIT ausgegebener Norm sowie wegen ihrer Detailliertheit und klaren Struktur kann die Norm möglicherweise als Vorbild für zukünftige konkretere Gesetze, Verwaltungsmaßnahmen oder verbindliche Normen dienen.[283]

9. Anwendbarkeit zentraler rechtlicher Begriffe auf das Cloud-Computing

Aufgrund der Fülle an unterschiedlichen Normen sollen an dieser Stelle die Ergebnisse der vorangegangenen Punkte hinsichtlich der begrifflichen Definition des Internetdienstanbieters und der persönlichen Daten einer kurzen Analyse unterzogen

263 Chin.: 个人信息管理者,
264 Vgl. *AQSIQ/SAC* (Fn. 226), S. 1 (Punkt 3.4).
265 Vgl. *AQSIQ/SAC* (Fn. 226), S. 2 (Punkt 4.1.3); *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 3.
266 Chin.: 个人信息获得者.
267 *AQSIQ/SAC* (Fn. 226), S. 1 (Punkt 3.5).
268 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.1.4).
269 Vgl. *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 3.
270 Chin.: 第三方测评机构.
271 Vgl. *AQSIQ/SAC* (Fn. 226), S. 1 (Punkt 3.6), S. 3 (Punkt 4.1.5); *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 3.
272 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2); *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 3 f.
273 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2 a, b).
274 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2 c).
275 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2 d).
276 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2 e, f).
277 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2 g).
278 Vgl. *AQSIQ/SAC* (Fn. 226), S. 3 (Punkt 4.2 h).
279 Vgl. *AQSIQ/SAC* (Fn. 226), S. 4 (Punkt 5.3.7).
280 Vgl. *AQSIQ/SAC* (Fn. 226), S. 5 (Punkt 5.5.1).
281 Vgl. *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 5.
282 Vgl. *Daniel Cooper/Eric Carlson/Scott Livingston* (Fn. 228) S. 3; *Graham Greenleaf/George Yijun Tian* (Fn. 231), S. 6.
283 Cooper/Carlson/Livingston sehen bspw. die konkrete Möglichkeit, dass verbindliche Normen in den nächsten Jahren erlassen werden könnten; vgl. *Daniel Cooper/Eric Carlson/Scott Livingston* (Fn. 228) S. 2.

und zusammengefasst sowie die Anwendbarkeit dieser Definitionen auf das Cloud-Computing geprüft werden, bevor im folgenden Abschnitt die Umsetzung des Datenschutzes betrachtet werden soll.

9.1 Anwendbarkeit des Begriffs des Internetdienstanbieters

In der chinesischsprachigen Literatur wird der allgemeine Begriff des „Internet Service Providers (ISP)" durch die Begriffe „Internet Access Provider (IAP)", „Internet Plattform Provider (IPP)" und „Internet Content Provider (ICP)" differenziert.[284] Der IAP sorgt lediglich für die technische Anbindung der Endgeräte des Kunden mit dem Internet. Er bietet dabei selbst keinerlei Inhalte oder Daten an. Der IPP bietet internetbasierte Software-Strukturen an in Form von Foren-, E-Mail- oder Blog-Software. Er gibt gleichzeitig dem Anwender die Möglichkeit, seine Dienste zu nutzen und mit eigenen Inhalte und Daten zu speisen. Der ICP schließlich bietet selbst (eigene oder fremde) Inhalte im Internet an, die von Dritten genutzt werden können. Der Unterschied zwischen IPP und ICP liegt insbesondere in der verstärkten redaktionellen Arbeit des ICP, was ihn grundsätzlich stärker für die von ihm angebotenen Inhalte verantwortlich macht.[285] Aufgrund der unterschiedlichen Aufgabenbereiche der verschiedenen ISP entstehen unterschiedliche rechtliche Pflichten.[286]

Eine ähnliche Unterteilung wie in der chinesischen Literatur ist auch in der deutschen Literatur üblich, allerdings ist die Trennung der Begriffe weniger scharf. So findet sich eine gleichwertige, allerdings nicht abschließende Unterteilung von „Telemediendiensten" in „Webseitenbetreiber [sowie] Access-, Host- und Contentprovider"[287]. An anderer Stelle werden Internet-Service-Provider mit Internet-Access-Providern gleichgestellt, werden jedoch wiederum in „Netwerk-Provider", „Webspace-Provider", „Content-Provider" und „Application-Service-Provider" unterteilt.[288] In der Tat überschneiden sich in der Praxis die Aufgaben und Dienstleistungen konkreter Internetdienstanbieter häufig und lassen sich nicht ausschließlich einer der o.g. Arten zuordnen.

Ein Anbieter von Cloud-Services ist wohl am ehesten als IPP im Sinne der chinesischen Literatur zu betrachten, als ein Anbieter also, der seinen Nutzern eine bestimmte Software-Plattform bereitstellt, dessen Dienstleistung jedoch über das bloße Bereitstellen einer Internetverbindung hinausgeht aber weniger stark auf eine Bereitstellung von redaktionell aufbereiteten Inhalten fokussiert ist.

Die verschiedenen administrativen Bestimmungen bieten sehr unterschiedliche Begrifflichkeiten. In den IntDienstlM von 2000 findet sich eine Definition von „Internetinformationsdienstleistungen"[289], wenn es heißt, dass als Internetdienstanbieter zu verstehen ist, wer Kunden[290] über das Internet Informationsdienstleistungen anbietet.[291] Eine weitergehende Konkretisierung dieser Definition erschöpft sich jedoch in der Unterteilung von solchen Dienstleistungen in kommerzielle und nicht-kommerzielle Angebote.[292]

WANG Shengming weist darauf hin, dass auch in den chinesischen Gesetzesnormen eine Vielzahl von Begriffen nebeneinander verwendet wird. So sei neben dem im DelHaftG angeführten „Internetdienstanbieter (ISP)"[293] an anderer Stelle von „Content Service Provider"[294], „Internet Access Provider"[295] oder schlicht „Internetseitenbetreiber"[296] die Rede.[297]

Die erste Erwähnung und gleichzeitig Unterscheidung von Internetdienstleistungen findet sich in den FernmBest von 2000, in deren Anhang zwischen „Internetzugangsdienstleistungen"[298] und „Internetinformationsdienstleistungen"[299] unterschieden wird.[300] Ersteres ist offenbar als Bereitstellung einer physikalischen Anbindung an das Internet zu verstehen, während letzteres als Angebot von Diensten aufzufassen ist, die auf dem Austausch von Informationen über das Internet basieren. Jedenfalls legt die Unterscheidung nahe, dass die physikalische Anbindung an das Internet keine Informationsdienstleistung darstellt.

---

284 Vgl. z.B. *ZHAO Yun* (赵云), Grundlegende Analyse der Haftung von Dienstleistern bei Verletzungen der Privatsphäre im Internet (浅析网络隐私侵权中服务商的责任承担), in: Legal System and Society (法制与社会), Vol. 9, No. 3, Kunming 2008, S. 82–83; *PENG Wenhua* (彭文化), Study on Criminal Responsibility of ISP's Crimes (网络服务商之刑事责任探讨), in: Journal of Foshan University (Social Science Edition) (佛上科学技术学院学报 (社会科学版)), Vol. 22, No. 3, Foshan 2004, S. 55–59; oder *SHI Ying* (石莹), Über die gesetzliche Haftung von ISP bei Rechtsverletzungen im Internet (论ISP在网络侵权中的法律责任), in: Shandong Justice (山东审判), Vol. 6, Jinan 2005, S. 117–119.

285 Vgl. *ZHAO Yun* (Fn. 252), S. 82.

286 So sieht PENG den ICP als grundsätzlich stärker für Inhalte Dritter in der strafrechtlichen Verantwortung. SHI liefert zwar eine begriffliche Trennung der verschiedenen Arten von ISP, bemerkt jedoch auch, dass oftmals mehrere Aufgaben von demselben Anbieter übernommen werden; vgl. *PENG Wenhua* (Fn. 252) und *SHI Ying* (Fn. 252).

287 *Marian Alexander Arning/Nils Christian Haag* (Fn. 37), Rn. 42.

288 Vgl. Stichwort „Internet-Service-Provider (ISP)" in *Insa Sjurts* (Hrsg.), Gabler Lexikon Medienwirtschaft, 2. Auflage, Heidelberg 2011, S. 306.

289 Chin.: 互联网信息服务.

290 Chin.: 用户.

291 Vgl. § 2 Abs. 2 IntDienstlM.

292 Vgl. § 3 IntDienstlM.

293 Chin.: 网络服务提供者.

294 Chin.: 内容服务提供者.

295 Chin.: 互联网接入服务提供者.

296 Chin.: 网站经营者.

297 Vgl. *WANG Shengming* (Fn. 56), S. 189.

298 Chin.: 互联网接入服务.

299 Chin.: 互联网信息服务.

300 Vgl. FermBest, Anhang: Punkt II, Unterpunkte 7 und 8.

Das DelHaftG baut auf den KommReBest von 2006 auf, die zwar in erster Linie den verbesserten Schutz des Urheberrechts zum Ziel hatten, in den §§ 20–23 jedoch bereits unterschiedliche Ausprägungen von Internetdienstleistungen definieren und mit unterschiedlichen Haftungsregelungen versehen.[301] Die Tätigkeit eines Cloud-Dienstleisters ist nach diesen Bestimmungen am ehesten als „Dienstleistung zur Datenspeicherung"[302] einzuordnen. Vor dem Hintergrund einer solchen Differenzierung in den KommReBest kann die Frage gestellt werden, welche konkreten Internetdienstleistungen unter den Begriff des ISP[303] in § 36 DelHaftG zu fassen sind. Für den Bereich des Cloud-Computings ist jedenfalls davon auszugehen, dass Cloud-Computing-Dienstleister unter den Begriff des ISP, wie er im DelHaftG verwendet wird, bzw. unter den Begriff des ICP[304] fallen. Ein Cloud-Dienst ist des weiteren allgemein als Internetinformationsdienstleistung[305] im Sinne der IntDienstlMarktR einzustufen.

9.2 Anwendbarkeit des Begriffs der persönlichen Daten

In der Literatur findet sich neben den grundsätzlich gleichwertigen chinesischen Begriffen *geren xinxi* und *geren shuju*[306] auch der Begriff *geren ziliao*[307]. In den rechtlichen Normen ist jedoch stets von *geren xinxi* die Rede. QI grenzt die Begriffe *xinxi* und *ziliao* dahingehend voneinander ab, dass *ziliao* – von QI als „Daten" übersetzt – nicht auf lediglich verschriftlichte Informationen begrenzt ist, während *xinxi* – als „Informationen" übersetzt – bereits für die Weiterverarbeitung aufbereitete Daten sind.[308] Der Begriff *geren xinxi* – hier als „persönliche Daten" übersetzt – hat sich jedoch offenbar im chinesischen Recht und in der neueren Literatur durchgesetzt und umfasst grundsätzlich jede Form der Aufzeichnung von Informationen.

Da das Konzept der „persönlichen Daten von Bürgern"[309] Einzug ins StGB gefunden hat und damit neben dem privatrechtlich kodifizierten Konzept der Privatsphäre zu stehen kommt, muss unweigerlich die Frage nach der Definition von persönlichen Daten gestellt werden. Das deutsche BDSG definiert personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)"[310]. Es liegt also der Fokus auf einer durch die jeweiligen personenbezogenen Daten ermöglichten Bestimmbarkeit, d.h. Identifizierbarkeit der entsprechenden Person.[311]

In den „Regulierungen zur Administration von Dienstleistungen von elektronischen Nachrichten im Internet" von 2000 (IntNachrDienstlR) taucht der Begriff der „persönlichen Daten"[312] bereits auf, wird jedoch nicht weiter konkretisiert.[313] Die Veröffentlichung von persönlichen Daten an Dritte ist demnach ohne die Zustimmung des Betroffenen nicht erlaubt und wird von den lokalen Telekommunikationsregulierungsbehörden verfolgt.[314] Für Schäden oder Verluste des Betroffenen ist nach dem Gesetz die Haftung zu übernehmen.[315]

Es bleibt also zunächst ungeklärt, welche Daten als persönlich anzusehen sind und welche nicht. Insbesondere ein häufiger Streitfall sind Adress- und sonstige Kontaktdaten, die Gegenstand eines regen Datenhandels sind. Zum einen lässt sich für Adressdaten eine gewisse Öffentlichkeit nicht absprechen, da sie für den Einzelnen eine Grundlage für die Teilhabe am gesellschaftlichen Leben darstellen. Auf der anderen Seite wird durch die Veröffentlichung von Adressdaten gerade ein wichtiger Aspekt des Datenschutzes ausgehebelt, nämlich die Privatsphäre von Einzelpersonen zu schützen. Andere persönliche Daten können als sensibler und damit prinzipiell schutzbedürftiger angesehen werden.[316] Man denke an Angaben zum Einkommen oder zum Anstellungsverhältnis. Ein besonders hoher Schutz dürfte für Daten gelten, die intimste persönliche Verhältnisse angeben, wie beispielsweise die sexuelle Orientierung oder religiöse Anschauungen.[317] Offensichtlich ist diesbezüglich eine einheitliche und klare Definition des Begriffs der persönlichen Daten notwendig.

Bereits bei der Diskussion des strafrechtlichen Schutzes von persönlichen Daten wurde auf die

---

301 Dies sind nach WANG Shengming Anbieter von „Access Services" (接入服务), von „Caching Services" (缓存服务), von „Dienstleistungen zur Datenspeicherung" (信息存储空间服务) sowie „Such- und Linkaggregationsdienste" (搜索和链接服务); vgl. *WANG Shengming* (Fn. 56), S. 187 f.; KommReBest, §§ 20–23; *HE Jian* (Fn. 119), 52.

302 Chin.: 信息存储空间服务.

303 Chin.: 网络服务提供者.

304 Chin.: 内容服务提供者.

305 Chin.: 互联网信息服务.

306 Chin.: 个人信息 (wörtl.: „persönliche Informationen") bzw. 个人数据 (wörtl.: „persönliche Daten"). S. zu diesem Begriffspaar die Anmerkungen in Fn. 59.

307 Chin.: 个人资料 (wörtl.: „persönliches Informationsmaterial").

308 Vgl. *QI Aimin* (Fn. 55), S. 3 f.

309 Chin.: 公民个人信息.

310 § 3 Abs. 1 BDSG.

311 Die Definition des BDSG wird dabei weit interpretiert, so dass auch für sich genommen nicht personenbezogene Daten, die aber durch Zusammenführung mit anderen Daten eine Identifizierung ermöglichen, zu personenbezogenen Daten werden können; vgl. *Marian Alexander Arning/Nils Christian Haag* (Fn. 37), Rn. 16.

312 Chin.: 个人信息.

313 Vgl. § 12 IntNachrDienstlR.

314 Vgl. § 19 IntNachrDienstlR i.V.m. § 12 IntNachrDienstlR.

315 Vgl. § 19 IntNachrDienstlR.

316 Vgl. *SHEN Yuzhong* (Fn. 79), S. 86.

317 Gleichwohl wird auch angemerkt, dass eine Einteilung von Daten nach deren Sensibilität wenig sinnvoll erscheint, da es stets auf den konkreten Kontext ankommt, in dem ein bestimmtes Datum verwendet wird, und selbst ein grundsätzlich wenig sensibles Datum wie ein Name allein durch die Verwendung in bestimmten Zusammenhängen zu einem sensiblen Datum werden kann; vgl. bspw. *Spiros Simitis* (Fn. 45), S. 402.

strittige Frage eingegangen, ob nur solche persönlichen Daten einen strafrechtlichen Schutz genießen, die auch die Privatsphäre des Datensubjekts betreffen. Die StärkDatSchBeschl bietet eine Formulierung, die dieser Frage noch einmal Zündstoff liefert, wenn sie persönliche Daten als solche Daten bezeichnet, „die geeignet sind, Rückschlüsse auf die persönliche Identität von Bürgern zu ziehen, und die die persönliche Privatsphäre von Bürgern betreffen."[318] Die Formulierung lässt offen, ob sie logisch konjunkt oder disjunkt zu verstehen ist, ob also persönliche Daten laut der Definition nur dann als solche zu verstehen sind, wenn sie die Privatsphäre betreffen. Während für die Regelung des StGB bereits ein Urteil auch zumindest Telefonnummern als persönliche Daten eingestuft und damit den engen Rahmen der Privatsphäre offenbar überschritten hat,[319] bleibt es die Aufgabe der Gerichte, in zukünftigen Urteilsentscheidungen die Formulierung in der StärkDatSchBeschl zu konkretisieren.

Auf verwaltungsrechtlicher Ebene haben 2012 die IntDienstlMarktR eine Definition für „persönliche Daten des Nutzers" geliefert, die derjenigen der StärkDatSchBeschl entspricht, jedoch den Passus zur Privatsphäre nicht enthält und auch Daten berücksichtigt, die erst durch Zusammenführung mit anderen Daten eine Identifizierung des Datensubjekts ermöglichen. Die TelIntDatSchR von 2013 schließlich geben zusätzlich konkrete Beispiele für „persönliche Daten des Nutzers", wie dessen Name, Geburtstag, Personalausweisnummer, Adresse, Telefonnummer, Nummer des Benutzerkontos sowie das Passwort und sogar Zeitpunkt und Ort des Zugriffs durch den Nutzer.

Für den Bereich des Cloud-Computing ist des weiteren von Interesse, ob auch die Verarbeitung und Nutzung von personenbezogenen Daten Dritter (d.h. nicht direkt dem Kunden des Cloud-Dienstleisters zuordenbare personenbezogene Daten) unter den jeweiligen Regelungsbereich einzuordnen sind und damit ebenfalls einen entsprechenden Schutz genießen. Abgesehen von der bereits oben angesprochenen Beschränkung auf Daten, die im Zuge der Ausübung der Amtspflichten bzw. der Erfüllung der Dienstleistungen erhoben worden sind, lässt sich dabei der Begriff der persönlichen Daten des StGB grundsätzlich generell auf alle personenbezogenen Daten von Bürgern (nicht aber von juristischen Personen[320]) beziehen. Damit sind jedenfalls auch Daten Dritter unter den Regelungsbereich zu fassen. Das DelHaftG gilt sogar ausdrücklich gleichermaßen für Internetdienstanbieter wie auch für Anwender[321], womit auch in diesem Falle ein Schutz von personenbezogene Daten Dritter besteht. Problematisch ist der Begriff der „persönlichen Daten des Kunden"[322], wie er in den IntDienstlMarktR und auch in den TelIntDatSchR verwendet wird.[323] Greenleaf sieht zwar die Definition in den IntDienstlMarktR grundsätzlich auf alle persönliche Daten des Nutzers anwendbar und nicht nur über die erhobenen,[324] jedoch erstreckt sich der Schutz nach dieser Formulierung offenbar nicht auf personenbezogene Daten Dritter. Die StärkDatSchBeschl beschränkt sich wiederum nicht auf Daten von Kunden, grenzt jedoch ihren Regelungsbereich auf „elektronische Daten" ein.

Zusammenfassend lässt sich sagen, dass der Begriff der persönlichen Daten im chinesischen Recht grundsätzlich auf natürliche Personen anwendbar ist. Persönliche Daten sind dabei solche Informationen, die eine Identifizierung eines Individuums ermöglichen. Legt man die Definition der StärkDatSchBeschl zugrunde, fallen darunter auch solche Daten, die erst durch Zusammenführung mit anderen Daten eine Identifizierung ermöglichen. Aufgrund der Rechtsprechung ist außerdem davon auszugehen, dass persönliche Daten grundsätzlich auch nicht die Privatsphäre betreffende Informationen wie Namen oder Kontaktdaten umfassen. Eine Unterscheidung in sensible und gewöhnliche Daten ist bisher lediglich in Industrienormen, jedenfalls aber nicht gesetzlich geregelt.

Dritter Teil: Umsetzung des Datenschutzes in der Cloud-Computing-Branche

10. Aufsichts- und Kontrollstrukturen

Im Falle der unerwünschten Veröffentlichung oder Weitergabe von personenbezogenen Daten liegt es regelmäßig am Betroffenen, den ISP oder die zuständigen Behörden über diesen Sachverhalt zu informieren. Dies setzt voraus, dass der Rechteinhaber als Geschädigter einen Überblick darüber hat, welche seiner Daten wo, durch wen und in welcher Weise rechtswidrig verarbeitet werden. Oft ist jedoch genau diese Nachvollziehbarkeit des konkreten Ortes, der konkreten Zeit und des konkreten Verursachers nicht gegeben.

Aus diesem Grunde ist eine Kontrolle des Datenschutzes durch neutrale Instanzen sowohl innerhalb der datenverarbeitenden Unternehmen wie auch auf übergeordneter Ebene durch unab-

---

318 § 1 Abs. 1 StärkDatSchBeschl.

319 Vgl. *CHANG Qing/ZHANG Li* (Fn. 139), S. 88.

320 Vgl. *ZHANG Mingkai* (Fn. 144), S. 825.

321 Chin.: 网络用户.

322 Chin.: 用户个人信息.

323 Vgl. §§ 11 und 12 IntDienstlMarktR; § 4 TelIntDatSchR.

324 Vgl. *Graham Greenleaf* (Fn. 186), S. 3.

hängige Kontrollorgane sinnvoll. Das deutsche Datenschutzrecht sieht sowohl einen dem Unternehmen eingegliederten Beauftragten für den Datenschutz[325] wie auch eine übergeordnete unabhängige Kontrollinstanz durch eine Aufsichtsbehörde[326] vor. In der chinesischen Literatur wird zum Teil die Etablierung einer solchen neutralen, von wirtschaftlichen Interessen und der Weisung durch Behörden unabhängigen Instanz gefordert.[327] Dieser Abschnitt beleuchtet die Aufsichts- und Kontrollmechanismen in China und ihre Umsetzung durch Kodifizierung und brancheninterne Regulierungsmechanismen.

10.1 Verwaltungsrechtlich kodifizierte Aufsichts- und Kontrollstrukturen

Abgesehen von der Möglichkeit, den juristischen Weg zu beschreiten, besitzt das Datensubjekt seit der StärkDatSchBeschl das gesetzlich verankerte Recht, Straftatbestände, die elektronische Daten betreffen, direkt bei den zuständigen Behörden anzuzeigen. Dies sind laut IntNachrDienstlR, IntDienstMarktRegR und TelIntDatSchR die lokalen Telekommunikationsbehörden, also die dem MIIT untergeordneten Behörden.[328] Die Behörden haben die Aufgabe, die im StGB definierten Tatbestände des Diebstahls bzw. des Verkaufs oder der rechtswidrigen Weitergabe „und andere Straftaten mit Bezug zu Daten im Internet[329] zu verhindern, aufzuhalten und zu untersuchen“[330]. Durch die Formulierung der StärkDatSchBeschl werden die genannten Straftaten jedenfalls als Antragsdelikt definiert, eine initiative Untersuchung eines Falles durch die Behörden wird jedoch ebenfalls nicht ausgeschlossen. Die TelIntDatSchR von 2013 heben die Pflicht der Behörden zur Aufsicht und auch Kontrolle der Maßnahmen zum Datenschutz des ISP hervor.[331] Bei einer Inspektion hat der ISP mit den Behörden zusammenzuarbeiten, allerdings darf die Inspektion die üblichen Arbeitsabläufe des ISP nicht behindern.[332] Der Betroffene soll sich offenbar jedoch zunächst an den ISP wenden, der in schwerwiegenden Fällen den Vorfall an die Behörden meldet. Inwieweit die Behörden auch von sich aus Inspektionen initiieren, ist aus den Regelungen der TelIntDatSchR jedenfalls nicht direkt ersichtlich.

Eine eindeutige innerbetriebliche Kontrollinstanz im Sinne eines Datenschutzbeauftragten sehen weder gesetzliche noch verwaltungsrechtliche Bestimmungen vor. Regelungen hierzu finden sich bisher lediglich in der 2012 erlassenen unverbindlichen Norm des MIIT in Form des genannten „Beauftragten für persönliche Daten“ und der „unabhängigen Drittorganisation“.[333] Cooper/Carlson/Livingston erwähnen zudem die Ankündigung der chinesischen Regierung, eine Beratungsstelle für den Datenschutz einzurichten, die möglicherweise die Selbstregulierung innerhalb der Branche bündeln und vertiefen wird.[334] Immerhin müssen Unternehmen seit den TelIntDatSchR von 2013 verbindliche interne Regeln zum Umgang mit personenbezogenen Daten aufstellen und und ein umfassendes Rechtemanagement einrichten, dass den Zugriff auf Daten auf bestimmte Mitarbeiter im Unternehmen beschränkt.[335] Die getroffenen Regelungen sind dem Nutzer mitzuteilen, zudem sind alle Zugriffe und Manipulationen von Daten zu protokollieren.[336]

10.2 Selbstregulierung der Internetbranche

Vor dem Hintergrund des zumindest bis zum Jahre 2009 schwachen gesetzlichen Schutzes von personenbezogenen Daten bei gleichzeitig zunehmendem Missbrauch von Daten und illegalem Datenhandel ist eine Umsetzung des Datenschutzes über Selbstregulierungsmechanismen von Branchenverbänden eine denkbare Alternative. Die in den Jahren 2005 entstandenen verschiedenen Entwürfe für ein chinesisches Datenschutzgesetz greifen diesen Gedanken auf, wenn sie die Umsetzung der rechtlichen Mechanismen über eine brancheninternen Selbstregulierung fordern oder eine parallele Aufsicht und Kontrolle durch Behörden und Branchenverbände definieren.[337] Da im chinesischen Recht bisher eine Aufsicht und Kontrolle über brancheninterne Strukturen in Form von Datenschutzbeauftragten nicht kodifiziert ist, ist eine Umsetzung über Selbstregulierungsabkommen wünschenswert.

Für die Verankerung umfassender Datenschutzstandards in Unternehmen spricht aus wirtschaftlicher Sicht die Tatsache, dass gerade innerhalb Cloud-Computing-Branche ein hohes Maß an Datensicherheit und Verlässlichkeit auch ein Wettbewerbsfaktor ist. Demgegenüber stehen jedoch die hohen Kosten für die Umsetzung eines umfassenden Datenschutzsystems im Unternehmen, zu dem

---

325 Vgl. §§ 4f, g BDSG.

326 Vgl. § 38 BDSG.

327 Vgl. bspw. *WANG Xuehao* (王学昊), Research on the Protection Modes of Personal Information and China's Legislation on Personal Information Protection (个人信息保护模式的比较研究及我国的立法选择), in: Internet Law Watch (互联网法律通讯), Vol. 7, No. 3, Beijing 2011, S. 97.

328 Vgl. § 19 IntNachrDienstlR; § 3 IntDienstMarktRegR; § 17 TelIntDatSchR; vgl. auch *Graham Greenleaf* (Fn. 186), S. 3.

329 Chin.: 其他网络信息违法犯罪行为.

330 § 10 Abs. 1 StärkDatSchBeschl.

331 § 17 TelIntDatSchR.

332 § 17 TelIntDatSchR.

333 S. dazu ausführlich Punkt 8.

334 Vgl. Daniel Cooper/Eric Carlson/Scott Livingston (Fn. 228), S. 1.

335 Vgl. § 13 TelIntDatSchR.

336 Vgl. § 8, 13 TelIntDatSchR.

337 S. dazu ausführlich Punkt 11.2.

unter anderem ein konsequentes Rechtemanagement, sichere Verschlüsselungsalgorithmen etc. gehören. Dieser Abschnitt widmet sich der Frage, inwiefern die existente Selbstregulierung der chinesischen Internetbranche Strukturen für den Schutz personenbezogener Daten bietet.

10.2.1 Regulierung über brancheninterne Abkommen

Effektive Mechanismen zur Wahrung von Datenschutz sind für Unternehmen stets mit Kosten verbunden. Weil die Implementierung solcher Mechanismen nur indirekt und jedenfalls nicht kurzfristig mit einer Umsatzsteigerung verbunden sind, zögern viele Führungskräfte in Internetsicherheit zu investieren.[338] Höhere Sicherheitsanforderungen richten sich dabei nicht nur gegen Angriffe von außen, beispielsweise durch Hacker, sondern gelten auch unternehmensintern. Oft sind es zudem die Mitarbeiter der Unternehmen, die am illegalen Handel mit Daten beteiligt sind, nicht zuletzt, da es an funktionellen internen Rechtezuweisungsmechanismen fehlt, die nur bestimmten Personen einen Zugang zu bestimmten Daten erlaubt.[339] Der Schutz der Daten muss sich also auch nach innen richten, was neben einer umfassenden Sicherung von Daten durch Verschlüsselung oder andere Verfahren auch eine klar strukturierte und konsequente Rechteverwaltung innerhalb der Unternehmen notwendig macht.

Trotz der vergleichsweise hohen Kosten, die mit der Umsetzung eines solchen effektiven Datenschutzes verbunden sind, ist zunächst davon auszugehen, dass Unternehmen, die Daten Dritter verarbeiten und speichern, von höheren Sicherheitsstandards profitieren, da für ihre Kunden und Nutzer höhere Sicherheitsstandards als Qualitätsmerkmal gelten können und damit ein wichtiges Merkmal zur Abgrenzung von der Konkurrenz darstellen. Dass die Umsetzung höherer Sicherheitsstandards grundsätzlich im Interesse vieler Unternehmen auch im chinesischen Internetsektor ist, zeigt die Vereinbarung von Selbstregulierungsabkommen innerhalb der Branche. Als Beispiel sei das „Selbstregulierungsabkommen der Internetbranche in China" genannt, das von der Internet Society of China (ISC)[340] im Jahr 2002 aufgesetzt worden ist.[341] Die ISC ist dem China Internet Network Information Center (CNNIC)[342] untergeordnet, das wiederum dem MIIT unterstellt ist.[343]

In diesem Abkommen verpflichten sich die Unterzeichner dazu, „Kundendaten geheim zu halten und Daten des Kunden nicht für Aktivitäten zu nutzen, die die [vertraglichen] Vereinbarungen mit dem Kunden nicht betreffen, oder unter Zuhilfenahme ihrer technischen oder anderweitigen Überlegenheit die legalen Rechte von Verbrauchern oder Kunden verletzen"[344]. Neuere ISC-Abkommen für besondere Teilbranchen, jedoch bisher nicht für den Cloud-Computing-Bereich, enthalten auch konkretere Regelungen zum Datenschutz.[345] Den bestehenden Abkommen mangelt es jedenfalls an konkreten, effektiven Sanktionen gegen die Unterzeichner im Falle der Verletzung der Abkommen und an Anspruchsgrundlagen des Geschädigten gegenüber den Unternehmen.[346] Die Abkommen können daher nicht ein fundiertes Regelwerk zum Datenschutz auf rechtlicher Basis ersetzen.

10.2.2 Regulierung über lokale Datenschutzerklärungen

Neben brancheninternen, unternehmensübergreifenden Abkommen kann auch der Anbieter einer Cloud- oder anderen internetbasierten Dienstleistung eine eigene Erklärung zu seiner Datenschutzpolitik abgeben. Einer kurzen Analyse zu unterziehen sind daher auch die Datenschutzerklärungen, die von einzelnen Betreibern auf ihren Internetseiten genannt werden. Dabei soll hier auf bereits existente Studien zurückgegriffen werden.

XU Jinghong kommt zu dem Ergebnis, dass in vielen Fällen eine solche Erklärung zwar vorhanden, aber inhaltlich wenig aussagekräftig gestaltet ist. Insbesondere kritisiert XU, dass auf vielen chinesischen Internetseiten Datenschutzerklärungen an einer nicht

---

338 Vgl. *YIN Pumin,* Protecting Personal Information: Curbing Personal Information Theft and Trading, in: Beijing Review, May 17, Beijing 2012, S. 20.

339 Vgl. *YIN Pumin* (Fn. 288), S. 20 f.

340 Chin.: 中国互联网协会.

341 Vgl. *JIANG Ge* (Fn. 142), S. 646; *HONG Hailin* (Fn. 4), S. 161; JIANG gibt hier offenbar fehlerhafterweise ein anderes Jahr und eine andere Fundstelle an.

342 Chin.: 中国互联网络信息中心.

343 Durch diese Konstruktion kann offenbar jedenfalls nicht von einer unabhängigen brancheninternen Selbstregulierung gesprochen werden, da eine gewisse behördliche Kontrolle zu vermuten ist; vgl. *WANG Xuehao* (Fn. 278), S. 101.

344 § 8 Selbstregulierungsabkommen der Internetbranche in China (中国互联网行业自律公约) vom 26. März 2002 (InternetSelbstRegAbk), <http://www.isc.org.cn/hyzl/hyzl/listinfo-15599.html> eingesehen am 30. Juni 2013. XU Jinghong kritisiert die im Abkommen fehlende nähere Bestimmung dieser „legalen Rechte"; vgl. *XU Jinghong* (徐敬宏), Self-Discipline of Internet Industry to Protect the Right of Internet Privacy: Actualities, Problems and Countermeasures (我国网络隐私权的行业自律保护: 现状、问题与对策), in: Library and Information (图书与情报), Vol. 5, Lanzhou 2009, S. 81.

345 So ist nach den §§ 9 und 10 des Selbstregulierungsabkommen von Softwaredienstleistungen für internetfähige Endgeräte (互联网终端软件服务行业自律公约) vom 1. August 2011 (InternetSoftwareSelbstRegAbk), <http://www.isc.org.cn/hyzl/hyzl/listinfo-15616.html> eingesehen am 30. Juni 2013, das Erheben, Speichern und Verarbeiten von personenbezogenen Daten der Nutzer ohne deren Einwilligung oder über das erforderliche Ziel hinaus sowie die Weitergabe von personenbezogenen Daten an Dritte verboten. Zudem sind Schutzmechanismen einzurichten, die die unerwünschte Veröffentlichung oder Weitergabe von Daten verhindern.

346 Vgl. *XU Jinghong* (Fn. 294), S. 81.

offensichtlichen Stelle stehen, inhaltlich schwammig oder fehlerhaft sind sowie dem Seitenbetreiber Rechte einräumen, die eigentlich dem Nutzer zuerkannt werden sollten.[347] XUs Kritik kann durch eine Studie von ZHOU Tao bestätigt werden. Auch hier kann gezeigt werden, dass nur in 60,78 % der in der Studie berücksichtigten Internetseiten die Datenschutzerklärung an einer prominenten und leicht zu erreichenden Stelle aufgeführt war,[348] nur in 31,4 % der Fälle wurde eine Weitergabe von personenbezogenen Daten an Dritte ohne die Zustimmung des Betroffenen ausgeschlossen.[349] Eine neuere Studie, die die Fair Information Practices von Internetseiten untersucht hat, kommt zu dem Ergebnis, dass nur 55 % der untersuchten Seiten überhaupt eine Datenschutzerklärung anboten, 32 % klärten über die Daten auf, die von den Seitenbetreibern verarbeitet werden. Immerhin 53 % der berücksichtigten Seiten wiesen nach der Studie in ihrer Datenschutzerklärung auf die Weitergabe der Daten an Dritte hin, aber nur 43 % gaben dem Betroffenen eine Option, der Weitergabe zuzustimmen bzw. diese abzulehnen. Nur 19 % der untersuchten Seiten boten dem Nutzer eine Möglichkeit, über die Nutzung seiner Daten durch den Seitenbetreiber zu entscheiden.[350] Insgesamt ergeben die verschiedenen Studien ein durchwachsenes Bild, was das Vorhandensein sowie die Qualität der Datenschutzerklärungen betrifft.

Die schwachen Regulierungen, die sich die Seitenbetreiber selbst auferlegen, lassen ein begrenztes Interesse der Branche vermuten, den Kunden eine ausreichend hohe Sicherheit bezüglich ihrer personenbezogenen Daten zuzugestehen. XU Jinghong begründet dies mit einem nur gering ausgeprägten Bewusstsein für Datenschutz unter den Nutzern solcher Internetdienste sowie mit der schwachen Durchsetzungskraft der bisherigen Gesetzgebung. Außerdem führt XU das Fehlen einer neutralen Kontrollinstanz als Ursache an.[351]

Zum gegenwärtigen Zeitpunkt fehlt es jedenfalls an einer zentralen unabhängigen Kontrollinstanz, die auch aktiv Überprüfungen zum Datenschutz einleitet. Trotz positiver Entwicklungen hinsichtlich datenschutzrelevanter Regelungen können brancheninterne Selbstregulierungsabkommen einen gesetzlich verankerten Kontrollmechanismus nicht ersetzen. Wenn in Unternehmen zudem bereits an der Einrichtung von ausreichenden Sicherheitsmechanismen gespart wird, da diese keine direkten Profite generieren, oder Mitarbeiter selbst in Adress- und Datenhandel involviert sind,[352] wird eine Sanktionierung durch die Branche selbst wohl nur schwer umsetzbar sein. Für die Etablierung eines funktionierenden Datenschutzregimes ist daher eine gesetzliche Kodifizierung der Aufsichts- und Kontrollstrukturen unbedingt erforderlich.[353]

11. Vorschläge und Gesetzesinitiativen im Datenschutz

Insbesondere wegen der zu erwartenden raschen Entwicklung im Bereich des Cloud-Computings und des noch nicht abgeschlossenen Prozesses der Kodifzierung datenschutzrechtlicher Normen ist es sinnvoll, einen Blick auf einige rechtstheoretische Entwicklungen im Bereich des Datenschutzes zu werfen. Als letzter Punkt sollen daher zum einen verschiedene Gesetzesinitiativen mit Bezug zum Datenschutz sowie alternative wissenschaftliche Debatten zur rechtlichen Einordnung des Datenschutzes kurz vorgestellt werden. Dabei erhebt dieser Abschnitt keinen Anspruch auf Vollständigkeit, sondern zeigt lediglich facettenhaft unterschiedliche Ansätze auf.

Das Bewusstsein für die Notwendigkeit eines umfassenden Datenschutzes hat zu verschiedenen Versuchen geführt, den Schutz personenbezogener Daten in strukturierter Form zu kodifizieren. Insbesondere drei Ansätze sind dabei herauszustellen, die alle aus dem Jahr 2005 stammen: zum einen der Entwurf eines Zivilgesetzbuches, der unter der Federführung von WANG Liming entstanden ist und der einen besonderen Abschnitt zum Datenschutz enthält, zum anderen ein Entwurf für ein Datenschutzgesetz von QI Aimin sowie ein weiterer Entwurf für ein Datenschutzgesetz einer Expertengruppe unter der Leitung von ZHOU Hanhua.

11.1 Kodifizierung des Datenschutzes im besonderen Teil eines zukünftigen Zivilgesetzbuches

Aus dem Jahr 2005 stammt ein umfassender Entwurf für ein Zivilgesetzbuch einer Gruppe Rechtswissenschaftler um WANG Liming, dessen

---

347 Bspw. führt XU Jinghong das Recht auf Berichtigung an, das nach seinen Untersuchungen oft bei den Seitenbetreibern verbleibe; vgl. *XU Jinghong* (Fn. 294), S. 82.

348 Vgl. *ZHOU Tao* (周涛) A Study of Website Privacy Statements Based on Content Analysis Method (基于内容分析法的网站隐私声明研究), in: Journal of Hangzhou Dianzi University (Social Sciences) (杭州电子科技大学学报 (社会科学版)), Vol. 5, No. 3, Hangzhou 2009, S. 14.

349 Vgl. *ZHOU Tao* (Fn. 298), S. 15.

350 Vgl. *HUANG Yuanyuan/XIE En/ZHANG Tao* (黄缘缘/谢恩/张涛), A Study on Fair Information Practices (FIPs) of China E-Commerce Websites (我国电子商务网站 FIPs 实施现状研究), in: Chinese Journal of Management (管理学报), Vol. 8, No., Wuhan 2011, S. 1197. Die Studie von Huang/Xie/Zhang befasst sich in erster Linie mit Internetangeboten im E-Commerce-Bereich, möglicherweise ist im Bereich des Cloud-Computing eine höhere Bereitschaft gegenüber Datenschutz- und Datensicherheitsvorkehrungen gegeben, da dieser Dienstleistungsbereich sich gerade auf den Transfer von Daten gründet.

351 Vgl. *XU Jinghong* (Fn. 294), S. 82.

352 Vgl. *YIN Pumin* (Fn. 288), S. 20 f.; *FU Xia* (Fn. 135), S. 111.

353 Als zusätzliche Kontrollstruktur wird in der Literatur außerdem unter anderem ein Zertifizierungssystem durch neutrale Drittorganisationen favorisiert; vgl. bspw. *WANG Xuehao* (Fn. 278), S. 97 f.

Teil zu den Persönlichkeitsrechten von YANG Lixin und MA Te[354] verfasst worden ist. Der Entwurf ordnet den Schutz persönlicher Daten[355] unter das Recht auf Privatsphäre ein.[356] Der Entwurf verfolgt das Prinzip der Zustimmung des Betroffenen,[357] der außerdem über das Ziel der Erhebung, die Weitergabe und den Umfang der Veröffentlichung zu unterrichten ist. Der Betroffene besitzt das Recht auf Einsicht, Änderung und Aktualisierung seiner Daten.[358] Ohne die Einwilligung des Datensubjekts dürfen keine persönlichen Daten vom Datenverarbeiter veröffentlicht oder weitergegeben werden.[359] Der Entwurf sieht außerdem eine Regelung für Internetseitenbetreiber vor, die dafür Sorge zu tragen haben, dass keine Daten Dritter ohne deren Erlaubnis veröffentlicht oder übertragen werden.[360]

Als Teil eines zukünftigen Zivilgesetzbuches können die Regelungen zum Datenschutz lediglich von grundsätzlicher Natur sein. Konkretere Regelungen müssen spezialgesetzlich normiert werden. Die Einordnung des Datenschutzes unter das Recht auf Privatsphäre wirft zudem zum einen die bereits oben erörterte Frage auf, ob der Schutz persönlicher Daten stets auch einen Schutz der Privatsphäre darstellt. Zum anderen kann eine privatrechtliche Kodifizierung des Datenschutzes grundsätzlich nicht auch auf die Datenverarbeitung durch öffentliche Stellen angewandt werden.

11.2 Umsetzung als eigenständiges Datenschutzgesetz

Die Entwürfe von QI Aimin und ZHOU Hanhua für ein chinesisches Datenschutzgesetz folgen einer ähnlichen Struktur: Nach einer Definition von Begriffen und grundlegenden Prinzipien (wie Einwilligung des Datensubjekts, Konkretisierung des Verwendungsziels, Grundsatz der Zweckbindung) folgen in einem zweiten Abschnitt Regelungen für die Verarbeitung und Nutzung personenbezogener Daten für staatliche Behörden und in einem dritten Abschnitt für sonstige Datenverarbeiter. ZHOU schließt dabei natürliche Personen, die Daten privat verarbeiten, und kleine Unternehmen mit geringen Datenvolumina von den Regulierungen aus.[361] Beide gewähren zudem dem Datensubjekt das Recht, über die erhobenen Daten Auskunft zu erhalten, was bei QI auch Angaben über Herkunft und Empfänger der Daten einschließt.[362] ZHOU gesteht dem Datensubjekt überdies das Recht auf Korrektur und auf Widerruf der Verarbeitung (d.h. Sperrung) zu.[363] Beide Entwürfe verfolgen ein offizielles Registrierungs- und Zertifizierungssystem für nichtstaatliche Stellen.[364] Die Umsetzung der im Gesetz vorgesehenen Regelungen soll in beiden Entwürfen über eine brancheninterne Selbstregulierung geschehen.[365]

ZHOU widmet der Durchsetzung und rechtlichen Haftung einen eigenständigen Teil in seinem Entwurf, in dem er die zuständigen Behörden, die rechtliche Durchsetzung im Schadenfall sowie verwaltungs- und strafrechtliche Haftungsbestimmungen anführt.[366] QIs Entwurf enthält auffallend viele Ausnahmen zu den angegebenen Regelungen.[367] Zudem gelten nach seinem Entwurf für nicht-staatliche Stellen viele der grundsätzlichen Regelungen für staatliche Stellen entsprechend, was hinsichtlich der grundsätzlich geringeren Befugnis von nichtstaatlichen Stellen, was die Datenerhebung betrifft, möglicherweise problematisch ist. So soll die Ausnahme, Daten an eine andere Stelle weiterzugeben, wenn dies für eine oder beide Seiten für die Ausübung ihrer Arbeit notwendig ist, auch für nichtstaatliche Stellen gelten.[368] Der Entwurf von ZHOU ist sehr viel detaillierter als derjenige QIs und kann als umfassendes Datenschutzgesetz betrachtet werden, auch wenn HONG (2007) bei ZHOU beispielsweise das Fehlen des Rechts des Datensubjekts auf Löschung seiner Daten bemängelt.[369]

Inwieweit die angeführten Entwürfe in der zukünftigen Gesetzgebung umgesetzt werden, wird sich in der weiteren Entwicklung des Datenschutzrechtes in China zeigen. Festzuhalten ist jedoch das Vorhandensein einer thematisch breitgefächerten und offenen Diskussion zum Thema Datenschutz in der chinesischen Fachliteratur, die die Dringlichkeit der Kodifizierung eines Schutzes persönlicher Daten deutlich macht.

---

354 Die Namen der beiden Autoren schreiben sich im Original 杨立新 und 马特.

355 Chin.: 个人资料.

356 Vgl. *HONG Hailin* (Fn. 4), S. 174.

357 Vgl. *WANG Liming* et al. (Fn. 60), S. 158 (§ 369).

358 Vgl. *WANG Liming* et al. (Fn. 60), S. 160 (§ 370).

359 Vgl. *WANG Liming* et al. (Fn. 60), S. 162 (§ 371).

360 Vgl. *WANG Liming* et al. (Fn. 60), S. 170 (§ 378).

361 Vgl. *HONG Hailin* (Fn. 4), S. 165.

362 Vgl. *QI Aimin* (齐爱民), Wissenschaftlicher Vorschlag eines Gesetzesentwurfs für ein Gesetz der VR China zum Schutz persönlicher Daten (中华人民共和国个人信息保护法示范法草案学者建议稿), in: Hebei Law Science (河北法学), Vol. 23, No. 6, Shijiazhuang 2005, S. 4 (§ 17 Abs. 1).

363 Vgl. *HONG Hailin* (Fn. 4), S. 169.

364 Vgl. *HONG Hailin* (Fn. 4), S. 166; *QI Aimin* (Fn. 310), S. 5 (§ 24).

365 Vgl. *HONG Hailin* (Fn. 4), S. 166; *QI Aimin* (Fn. 310), S. 5 (§ 29).

366 Vgl. *HONG Hailin* (Fn. 4), S. 166.

367 Bspw. soll eine Erhebung und Verarbeitung von Daten, die bereits veröffentlicht wurden und die Rechte des Datensubjekts nicht verletzten, grundsätzlich erlaubt sein; vgl. *QI Aimin* (Fn. 310), S. 5 (§ 26 Abs. 1 Satz 3).

368 Vgl. *QI Aimin* (Fn. 310), S. 3 (§ 12 Abs. 1 Satz 1) i.V.m. *QI Aimin* (Fn. 310), S. 5 (§ 28). Auch sollen nicht-staatliche Stellen auch für die Erreichung des vereinbarten Ziels nicht notwendige Daten erheben dürfen, wenn diese geeignet sind bspw. das „öffentliche Interesse" zu schützen; eine solche Kompetenz sollte jedoch grundsätzlich staatlichen Stellen vorbehalten sein; vgl. *QI Aimin* (Fn. 310), S. 5 (§ 26 Abs. 2 Satz 1).

369 Vgl. *HONG Hailin* (Fn. 4), S. 171.

Zusammenfassung der Ergebnisse

12. Fazit

Insbesondere bei der Inanspruchnahme von Cloud-Computing-Dienstleistungen für die Speicherung und Verarbeitung von personenbezogenen Daten Dritter ergeben sich rechtlich relevante Fragestellungen. Bei der Weitergabe personenbezogener Daten besteht für den Betroffenen ein erhöhtes Interesse an rechtlicher Sicherheit, da er nicht ohne weiteres nachvollziehen kann, in welcher Weise und an welchem Ort seine Daten letztendlich verarbeitet und gespeichert werden. Konkrete Regelungen zu einer Verarbeitung personenbezogener Daten im Auftrag, wie sie das deutsche BDSG bietet, gibt es jedoch bislang im chinesischen Recht nicht. Ebenso fehlt es an einem konsistenten Regelungswerk zum Datenschutz im Allgemeinen. Stattdessen ist eine Vielzahl von Einzelnormen aus verschiedenen Rechtsbereichen maßgeblich für den Schutz von personenbezogenen Daten auch im Bereich des Cloud-Computing. Die wichtigsten rechtlichen Grundlagen bieten dabei das DelHaftG, das StGB, die StärkDatSchBeschl sowie die IntDienstlMarktR i.V.m. den IntNachrDienstlR. Cloud-Computing-Dienstleister fallen nach chinesischem Recht unter den Begriff des Internetdienstanbieters und haben sich an entsprechende branchenspezifische Regelungen zu halten, die auch die Verarbeitung personenbezogener Daten betreffen. Durch die nur bedingt gegebene Passgenauigkeit der Begrifflichkeiten ergeben sich jedoch vor allem aus der Sicht des Datensubjekts einige rechtliche Lücken, die auch und gerade bei der Nutzung von Cloud-Computing-Diensten zum Tragen kommen.

Ein grundsätzliches Problem der rechtlichen Umsetzung des Datenschutzes im chinesischen Recht besteht in der fehlenden Anwendbarkeit von verfassungsrechtlich verankerten Grundrechten insbesondere auf privatrechtliche Zusammenhänge. Eine Ableitung von Persönlichkeitsrechten aus der chinesischen Verfassung ist grundsätzlich nicht möglich, stattdessen finden sich einzelne Persönlichkeitsrechte im Privatrecht positiviert, darunter auch das Recht auf Privatsphäre. Aufgrund des bisherigen Fehlens eines umfassenden Zivilgesetzbuches, dessen Aufgabe insbesondere die rechtliche Definition von Privatsphäre ist, bedarf die bisherige bloße Nennung des Rechts auf Privatsphäre im DelHaftG einiger Interpretation. Es besteht jedenfalls erhebliche Unklarheit, ob eine unerwünschte Veröffentlichung oder Weitergabe von personenbezogenen Daten stets als Verletzung des Rechts auf Privatsphäre gelten kann und insbesondere ob aus einer solchen Verletzung stets auch ein Anspruch auf Schadenersatz erwächst. Ein Schutz personenbezogener Daten kann daher nicht allein auf diesem privatrechtlichen Wege umfassend gewährleistet werden. Dem Erlass eines chinesischen Datenschutzgesetzes steht zudem die grundsätzliche rechtstheoretische Frage im Wege, welches Persönlichkeitsrecht als Grundlage für den Schutz personenbezogener Daten herangezogen werden kann und ob die bestehenden und bereits kodifizierten Persönlichkeitsrechte als eine Grundlage dienen können.

Die Diskussion in der Literatur offenbart eine tiefergehende Auseinandersetzung mit dem Thema Datenschutz seit Mitte der 2000er Jahre sowie in jüngster Zeit eine Infragestellung des früheren Ansatzes, den Schutz personenbezogener Daten unter das Recht auf Privatsphäre zu fassen. Verstärkt findet sich stattdessen die Ansicht, dass der Schutz personenbezogener Daten als eigenständiges Persönlichkeitsrecht ähnlich dem deutschen Recht auf informationelle Selbstbestimmung zu formulieren ist.

Betrachtet man die Fortentwicklung der Gesetzesnormen, so finden sich zunächst Einzelverordnungen in Form von Verwaltungsmaßnahmen für den Internet-Sektor, die sich insbesondere an ISP richten, sowie ab 2009 ein privatrechtlicher Schutz der Privatsphäre, der offenkundig auch in das öffentliche Recht und dort insbesondere in das Strafrecht hineinstrahlt und sich dort als Schutz von personenbezogenen Daten manifestiert. Inwieweit die akademisch geführte Diskussion über die Einordnung des Schutzes personenbezogener Daten sich im positiven Recht manifestieren, kann zum gegenwärtigen Zeitpunkt nicht abschließend geklärt werden. In jüngeren Gerichtsentscheidungen[370] wurde allerdings offenbar bereits von einer konzeptionellen Trennung des Begriffs der personenbezogenen Daten von dem rechtlichen Konstrukt der Privatsphäre ausgegangen.

Für das Datensubjekt ergeben sich unterschiedliche Wege der Rechtsdurchsetzung. Grundsätzlich besteht für den Betroffenen die Möglichkeit, gegen einen Cloud-Anbieter oder sonstigen ISP bei der durch diesen verursachten oder über dessen Internetplattformen erfolgten unerwünschten Veröffentlichung von personenbezogenen Daten auf der Grundlage des DelHaftG einen Anspruch auf Unterlassung und Schadenersatz zu erwirken. Das DelHaftG schützt durch seine besondere Behandlung der Verletzung des Rechts auf Privatsphäre im Internet jedoch auch den ISP insofern, als dieser erst dann für die durch die Rechtsverletzung entstandenen Schäden haftbar gemacht werden kann, wenn er schuldhaft der Aufforderung zur Entfernung der unerwünschten Daten nicht nachkommt.

---

[370] S. Fn. 145.

Neben dem privatrechtlichen Weg besteht für den Betroffenen die Möglichkeit einer strafrechtlichen Verfolgung der unerlaubten Veröffentlichung, Weitergabe oder Aneignung personenbezogener Daten. Hinsichtlich unerlaubter Veröffentlichung und Weitergabe können jedoch über das Strafrecht nur bestimmte Institutionen verfolgt werden. Es ist hier außerdem zu prüfen, ob die Daten im Rahmen der Erfüllung öffentlicher Aufgaben oder der Erbringung einer Dienstleistung durch die entsprechende Institution erhoben worden sind. Eine strafrechtliche Verfolgung wird überdies lediglich in so genannten schwerwiegenden Fällen eingeleitet. Handelt es sich um elektronische personenbezogenen Daten, kann der Betroffene aufgrund der StärkDatSchBeschl, die den Verkauf und die Weitergabe von elektronischen personenbezogenen Daten ausdrücklich verbietet, zudem gegen das Unternehmen vorgehen, das seine Daten widerrechtlich weitergegeben hat.

Seit den TelIntDatSchR wird dem Betroffenen immerhin ein Recht zur Einsicht und nachträglichen Änderung seiner Daten eingeräumt. Die Regelungen zur Sperrung oder Löschung der überlassenen Daten sind jedoch auch weiterhin unklar, so dass man hier jedenfalls nicht von klar definierten Rechten des Betroffenen sprechen kann. Das jede Datenverarbeitung zuvor der Zustimmung des Betroffenen bedarf kann inzwischen als anerkannter Grundsatz gelten, auch wenn die Art und Form der Zustimmung bisher nicht konkretisiert wurde. Bereits die IntDienstlMarktR definieren zudem die Durchsetzbarkeit der Sanktionierung dieses Grundsatzes durch das MIIT und untergeordnete Telekommunikationsbehörden. Obwohl die TelIntDatSchR einen großen Schritt hin zu einer umfassenden internen und externen Kontrolle durch entsprechende Schutzmechanismen machen, bleibt der Betroffene vermutlich weiterhin in erster Linie zunächst selbst für die Kontrolle über seine Daten verantwortlich.

Bei der besonders im Bereich des Cloud-Computing relevanten Weitergabe von Daten durch ein Unternehmen an eine andere Stelle zur Speicherung und Verarbeitung hat der Betroffene nach chinesischem Recht nur wenig Kontrollmöglichkeiten. Abgesehen von den privat- und strafrechtlichen Möglichkeiten, die grundsätzlich auf jede Stelle in der Verarbeitungskette anwendbar sind, gilt immerhin im Falle der Erhebung direkt beim Betroffenen ein Verbot der Weitergabe an Dritte ohne dessen Einwilligung. Unklar bleibt, ob das Datensubjekt über die Tatsache und den Umfang der Weiterverarbeitung seiner Daten sowie über die Identität der weiterverarbeitenden Stelle informiert werden muss und ob Daten, die über andere Kanäle als die direkte Erhebung erlangt wurden, ebenfalls einem Einwilligungsvorbehalt hinsichtlich der Weitergabe unterliegen. Positiv zu bewerten ist die Regelung der TelIntDatSchR, die immerhin eine Weitergabe von personenbezogenen Daten nur an solche Dritte erlaubt, die den rechtlichen Ansprüchen der Verarbeitung genügen.

Vor dem Hintergrund der politisch erwünschten Weiterentwicklung im Bereich des Cloud-Computing in China und der daher zu erwartenden Intensivierung der Nutzung von Cloud-Diensten sowohl im Inland wie auch auf internationaler Ebene wird das Bedürfnis nach einem an internationale Richtlinien angepassten Datenschutz für weitere Entwicklungen im chinesischen Recht sorgen. Hinweise auf solche Entwicklungen sind in bereits heute existierenden, vergleichsweise umfassenden Regelungen auf regionaler und branchenspezifischer Ebene sowie in Industrienormen zu finden. Auch in brancheninternen Selbstregulierungsabkommen scheint der Datenschutz stärkere Berücksichtigung zu finden. Die rege Diskussion sowohl auf wissenschaftlicher wie politischer Ebene und verschiedentliche Initiativen zum Erlass eines Datenschutzgesetzes zeugen zudem von einem erstarkten Bewusstsein für die Notwendigkeit der Umsetzung eines umfassenden Schutzes personenbezogener Daten.

Einem stärkeren Schutz stehen jedoch auch wirtschaftliche wie politische Interessen gegenüber. Ein höherer Datenschutz geht naturgemäß mit höheren Kosten für die Einrichtung von Schutz- und Kontrollmechanismen sowie mit begrenzterem Zugriff auf wirtschaftliche wie politisch interessante Informationen einher. Die Kodifizierung zukünftiger datenschutzrechtlicher Regelungen wird sich daher an der eingangs genannten Balance zwischen den verschiedenen Interessen von Bürgern, Wirtschaft und Staat ausrichten müssen. Welche Interessen dabei den Normierungsprozess stärker beeinflussen werden, muss die zukünftige Entwicklung zeigen.