Sonderdruck aus:

Verfassungsstaatlichkeit im Wandel

Festschrift für Thomas Würtenberger zum 70. Geburtstag

Herausgegeben von

Dirk Heckmann
Ralf P. Schenke
Gernot Sydow

Duncker & Humblot · Berlin 2013

Cloud Computing im Zeitgeist

Juristische Hürden, rechtspolitische Unwägbarkeiten, unternehmerische Gestaltung

Von *Dirk Heckmann*, Passau

I. Einleitung

Die „Cloud" kommt und sie verändert alles:[1] Sei es die IT-Organisation der Unternehmen und Behörden, das Verständnis von „Datenbesitz" und „Datenherrschaft" oder die Geschäftsmodelle großer Teile der IT-Branche. Cloud Computing revolutioniert z. B. die Arbeitsorganisation, indem Informationen in verteilten Systemen von Akteuren verarbeitet werden, die sich nicht kennen und doch einander vertrauen – und zwar weltweit. Gleiches gilt für die Bereitstellung und Nutzung von Applikationen. So fördert Cloud Computing die Globalisierung und prägt letztlich ein neues Verständnis der IT als „Geschäft auf Gegenseitigkeit". Umso stärker gilt es, die rechtliche Dimension[2] dieser innovativen Entwicklung im Auge zu behalten. Das geltende deutsche und europäische Datenschutzrecht kennt zwar Rahmenbedingungen für die sog. Auftragsdatenverarbeitung (zum Beispiel in § 11 BDSG). Diese sind auf das Konzept des Cloud Computing allerdings nur ansatzweise anwendbar. Umgekehrt formuliert: Wenn man die hohen rechtlichen, technischen und organisatorischen Anforderungen, die etwa § 11 Abs. 2 BDSG für die Auftragsdatenverarbeitung im Sinne eines klassischen IT-Outsourcing formuliert, „formaljuristisch" zum Maßstab an Cloud-Lösungen anlegt, beenden Datenschutz-Bedenken die Annäherung an solche Innovationen, ohne dass eventuelle Vorteile von Cloud Computing, nämlich Überle-

---

[1] So lautete das Credo auf der Cebit 2012. Einen Überblick über die rechtlichen, technischen und wirtschaftlichen Aspekte des Cloud Computing bietet *Heckmann*, in: Heckmann, jurisPK Internetrecht, 3. Aufl. 2011, Kap. 9, Rn. 577 ff.

[2] Es gibt nicht „das" Cloud Computing, so dass sich pauschale rechtliche Bewertungen verbieten. Dessen kennzeichnende Elemente (wie Flexibilität, Skalierbarkeit, Ressourcenteilung, Elastizität oder nutzungsorientierte Abrechnung) lassen sich mit unterschiedlichen Diensten und Services (Infrastructure as a Service, Software as a Service, Platform as a Service etc.) und unterschiedlicher Reichweite der Auslagerung von Daten und Diensten (Bereitstellungsformen: Public Cloud, Private Cloud, National Cloud, Community Cloud u. a.) mit entsprechender technischer Ausgestaltung und passenden Geschäftsmodellen verwirklichen. Ausführlich dazu vgl. *Hennrich*, CR 2011, 546 ff.

Zum Cloud Computing in der öffentlichen Verwaltung vgl. *Heckmann*, in: Hill/Schliesky, Innovationen im und durch Recht, 2010, S. 97 ff.; *ders.*, Der Bayerische Bürgermeister 9/2011, S. 302 ff.; *Maisch/Seidl*, VBIBW 2012, 7 ff.

gungen der Effizienz, der Wirtschaftlichkeit und auch der IT-Sicherheit, überhaupt Gehör finden. In diesem Sinne raten derzeit neben Datenschützern auch viele Anwaltskanzleien davon ab, personenbezogene Daten in eine „Cloud" auszulagern, weil das Haftungsrisiko unüberschaubar sei.[3] Das ist allerdings nicht die einzige Hürde, der sich Anbieter von Cloud-Lösungen stellen müssen. Die Geschichte technischer Innovationen zeigt immer wieder, dass es zu Beginn zahlreiche Widerstände, Hindernisse und vermeintlich unüberschaubare Risiken gibt, die sich solchen Veränderungen entgegenstellen. Aus Sicht anbietender Unternehmen sind das sog. „Sales Blocker", also Entwicklungs- und Vertriebshindernisse, die eine Etablierung selbst hoch nützlicher Produkte erschweren, was umso ärgerlicher erscheinen mag, je stärker sich das Unternehmen an einem internationalen Markt orientieren muss, auf dem auch die Produkte ausländischer Konkurrenz Abnehmer finden. Was aber sind die Sales Blocker beim Cloud Computing und gibt es umgekehrt auch Enabler? Mit dieser wissenschaftlich bislang nicht näher untersuchten Fragestellung befasst sich der Beitrag zu Ehren von Thomas Würtenberger, einem Wissenschaftler, der in seiner Forschung stets auch den Blick über die Grenzen der Rechtsdogmatik hinaus gerichtet hat, besonders im Hinblick auf die Einflüsse des Zeitgeistes auf die Rechtsentwicklung.

II. Beharrungstendenzen der Rechtsordnung

„Sales Blocker" ergeben sich beim Cloud Computing in erster Linie aus den Beharrungstendenzen juristischer Kreise gegenüber (technischen) Innovationen, insbesondere durch die Scheu mancher Juristen, das Recht zeitgemäß auszulegen und anzuwenden.

1. Technische Innovation trifft auf konservierendes (konservatives) Recht

Das BSI bezeichnet Cloud Computing als „das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz."[4] Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software."[5] Cloud Computing zählt

[3] Vgl. etwa die Stellungnahme des Deutschen Anwaltvereins gegenüber der EU-Kommission http://www.anwaltverein.de/downloads/Stellungnahmen-11/43-2011-SN-Cloud-Computing.pdf.

Kritisch auch *Weichert*, DuD 2010, 679; *Becker/Nikolaeva*, CR 2012, 170 ff.

[4] https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html.

[5] BSI Eckpunktepapier zum Cloud Computing, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-Cloud Computing-Anbieter.pdf?__blob=publicationFile.

im Kontext der informationstechnologischen Entwicklung, auf ihr beruhender IT-Angebote und entsprechender Geschäftsmodelle zu den herausragenden Innovationen des ersten Jahrzehnts im 21. Jahrhundert.[6] Auch wenn es aktuell noch relativ konturenlos erscheint (zum „hohen Abstraktionsniveau" der Cloud-Computing-Diskussion weiter unten IV.), wird die Fortschrittlichkeit des Cloud Computing nirgends bestritten. Im Gegenteil: Auch – und gerade – die Kritiker heben das Innovationspotential hervor.[7] Gerade hier knüpfen dann aber auch deren Bedenken an: Cloud Computing sei – zumindest in bestimmten Erscheinungsformen – rechtlich fragwürdig, nicht datenschutzkonform oder wegen unkalkulierbarer Haftungsrisiken nicht empfehlenswert.[8] Wenn man nach „Sales Blockern" (im Sinne von Hürden für den Absatz von Cloud-Computing-Angeboten) fragt, sind vorrangig die Beharrungstendenzen der Rechtsordnung zu nennen. Technische Innovation trifft auf konservatives Recht – und auf konservative Juristen.

Dies zeigt sich in aller Deutlichkeit bei der Auslegung der maßgeblichen Vorschrift des § 11 BDSG. Diese Norm regelt die Auftragsdatenverarbeitung und enthält auch die bislang für IT-Outsourcing-Verträge wesentlichen Anforderungen. Flankierend sind die §§ 4b, 4c sowie 9 BDSG und seine Anlage zu beachten.

2. Konventionelle Auslegung des § 11 BDSG

a) Sicherungsmechanismen für die Auftragsdatenverarbeitung (§ 11 BDSG)

Kommt es bei der Nutzung cloud-basierter Dienste – wie es regelmäßig der Fall sein wird – zur Verarbeitung personenbezogener Daten (§ 3 Abs. 1 BDSG), so ist im Verhältnis des Anwenders zum Diensteanbieter von einer Auftragsdatenverarbeitung i.S.d. § 11 BDSG auszugehen, bei der der Auftraggeber als „Herr der Daten" datenschutzrechtlich verantwortlich bleibt.[9] § 11 BDSG verlangt, dass in einem Cloud-Computing-Vertrag unter anderem Festlegungen hinsichtlich Art, Ort und Umfang der Verarbeitung der personenbezogenen Daten durch den Anbieter sowie Regelungen zum Schicksal der Daten im Fall der Beendigung des Vertrages als auch konkrete technische und organisatorische Maßnahmen zum Schutz der Daten gem. § 9 BDSG

[6] Zu den technischen Grundlagen des Cloud Computing vgl. *Heckmann*, in: Hill/Schliesky, Innovationen im und durch Recht, S. 97 ff.; *Maisch*, AnwZert-ITR 15/2009, Anm. 4; *Niemann/Hennrich*, CR 2010, 686 ff.

[7] Siehe beispielhaft die Darstellung zu dem Zweck des Cloud Computing bei *Weichert*, DuD 2010, 679.

[8] Vgl. *Weichert*, DuD 2010, 679 ff.

[9] *Schulz*, MMR 2010, 75 (78); *Pohle/Ammann*, CR 2009, 273 (277); *Maisch*, AnwZert-ITR 15/2009, Anm. 4; allgemein zu § 11 BDSG: *Ehmann*, in: Abel (Hrsg.), Praxiskommentar Bundesdatenschutzgesetz, 5. Aufl. 2009, S. 228 ff.; zur Auftragsdatenverarbeitung in der Kommunalverwaltung: *Lübking/Zilkens*, Datenschutz in der Kommunalverwaltung, 2. Aufl. 2008, Rn. 487 ff.

und seiner Anlage aufgenommen werden.[10] Dabei müssen dem Auftragnehmer die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes und der Datensicherheit – abgestimmt mit dem Auftraggeber auf die Bedürfnisse des konkreten Auftragsverhältnisses – vorgegeben und deren Realisierung vertraglich abgesichert werden.[11] Beim Cloud Computing gestaltet sich schon die konkrete Wiedergabe der Maßnahmen als schwierig. Dies gilt nach dem Verständnis vieler nationaler Datenschutzaufsichtsbehörden insbesondere für Public Clouds.[12]

Zu beachten ist weiterhin, dass die Unkenntnis vom Ort der Verarbeitung oder Speicherung der Daten beispielsweise durch technische Mittel wie geeignete Reporting- oder Monitoring-Tools mit einem entsprechenden Onlinezugriff für den Kunden vermieden werden könnte.[13] Diese Lösung dürfte technisch ohne übermäßige Schwierigkeiten umsetzbar sein, da die erforderlichen Informationen auf technischer Ebene ohnehin verfügbar sein müssen, um dem Kunden jederzeit Zugang zu den Daten zu ermöglichen.[14]

Mit Blick auf die Besonderheiten des Cloud Computing in weltweit verteilten Rechenzentren ist schließlich zu berücksichtigen, dass sich der Auftraggeber Gewissheit über die Gewährleistung des zu sichernden Schutzstandards verschaffen muss.[15] Dies kann schon bei der Auswahl des Anbieters, beispielsweise durch Heranziehung von Zertifizierungen qualifizierter Dritter[16] oder Informationen von Referenzkunden geschehen. Bei der Überwachung etwa durch entsprechend vereinbarte Berichtspflichten und regelmäßige Auditierungen des Auftragnehmers sowie durch ergänzende Kontrollrechte des Auftraggebers (vgl. § 11 Abs. 2 S. 2 Nr. 7, 9 BDSG).[17]

Insgesamt ist es unterdessen kaum vorstellbar, dass im Bereich der aktuell bekannten Cloud-Computing-Modelle die Formulierung eines IT-Outsourcing-Vertrages gelingen mag[18], der alle Anforderungen des § 11 Abs. 2 BDSG einhält. Im Übrigen ist eine strikte Daten- und Verfahrensherrschaft des Auftraggebers nach dem Geschäftsmodell des Cloud Computing weder möglich noch erwünscht.

[10] *Klinger*, AnwZert-ITR 25/2009, Anm. 3.

[11] *Klinger*, AnwZert-ITR 25/2009, Anm. 3; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 11 Rn. 41; *Gabel*, in: Taeger/ders. (Hrsg.), Kommentar zum BDSG, 2010, § 11 Rn. 44.

[12] *Niemann/Paul*, K&R 2009, 444 (449); auch der Nutzer des Cloud Computing weiß häufig gerade nicht, an welche geografischen Orte seine personenbezogenen Daten übermittelt werden, *Schulz*, MMR 2010, 75 (78).

[13] *Gabel*, in: Taeger/ders. (Hrsg.), Kommentar zum BDSG, 2010, § 11 Rn. 18; ebenfalls für eine hohe Verfahrenstransparenz: *Maisch*, AnwZert-ITR 15/2009, Anm. 4.

[14] *Reindl*, in: Taeger/Wiebe, Inside the Cloud – Neue Herausforderungen für das Informationsrecht, 2009, S. 444.

[15] *Gabel*, in: Taeger/ders. (Hrsg.), Kommentar zum BDSG, 2010, § 11 Rn. 33 ff.

[16] Vgl. *Maisch*, AnwZert-ITR 15/2009, Anm. 4.

[17] *Reindl*, in: Taeger/Wiebe, Inside the Cloud – Neue Herausforderungen für das Informationsrecht, 2009, S. 449.

[18] Sofern eine Auftragsdatenverarbeitung scheitert, richtet sich die erfolgende Datenübermittlung nach den Vorgaben des BDSG. Sie wäre dann nur beim Vorliegen einer konkreten (informierten) Einwilligung des Betroffenen oder einer gesetzlichen Ermächtigungsgrundlage zulässig; *Schulz*, MMR 2010, 75 (78).

b) Datenschutzniveau bei der Datenverarbeitung in Drittländern (§ 4b BDSG)

Mit Hinblick auf die weltweite Datenverarbeitung in der Cloud stellen sich Rechtsfragen der Anwendbarkeit nationaler Rechtsregime.

aa) Die Anwendbarkeit deutschen Datenschutzrechts richtet sich nach § 1 Abs. 5 BDSG. Für den EU-grenzüberschreitenden Datenverkehr normiert § 1 Abs. 5 S. 1 BDSG in Einklang mit Art. 4 der EU-Datenschutzrichtlinie das Sitzlandprinzip. Für auf den Anwendungsbereich der EU-Datenschutzrichtlinie beschränkte Cloud-Dienste bedeutet dies, dass das insoweit anzuwendende nationale Recht sich nicht nach dem Ort der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten richtet, sondern nach dem Recht des Ortes, an dem die hierfür verantwortliche Stelle ihren Sitz hat. Für ein in Deutschland ansässiges Unternehmen, das als Auftraggeber i.S.v. § 11 BDSG Cloud-Dienste in Anspruch nimmt, hat dies bei „europäischen Clouds" regelmäßig die Anwendung deutschen Datenschutzrechts zur Folge. Anders ist die Lage gemäß § 1 Abs. 5 S. 2 BDSG bei der Datenverarbeitung durch eine verantwortliche Stelle, die außerhalb des Anwendungsbereichs der EU-Datenschutzrichtlinie belegen ist.

Für die Frage, ob bei einer „innereuropäischen" oder „außereuropäischen" Cloud das Privileg der Auftragsdatenverarbeitung – im Unterschied zur Funktionsübertragung – angenommen werden kann, enthält § 3 Abs. 8 BDSG eine wichtige Weichenstellung. Eine Auftragsdatenverarbeitung liegt nach der Grundkonzeption des § 11 BDSG nur vor, wenn der Auftragnehmer (Cloud-Dienstleister) weisungsgebunden ist, d. h. ohne eigenen Wertungs- und Entscheidungsspielraum für den Auftraggeber (Cloud-Nutzer) tätig wird. Fehlt es hieran (bspw. weil dem Auftragnehmer die Daten für eigene Geschäftszwecke überlassen werden), so ist der Auftragnehmer als Dritter i.S.d. § 3 Abs. 8 S. 2 BDSG anzusehen. Die Datenverarbeitung durch einen Dritten ist jedoch nicht von § 11 BDSG erfasst und bedarf als sog. Funktionsübertragung eines eigenen Erlaubnistatbestandes gem. § 28 ff. BDSG. Nach der Konzeption des § 3 Abs. 8 BDSG ist als Dritter auch eine solche Stelle einzustufen – unabhängig von der Entscheidungsfreiheit –, die außerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie tätig wird.[19]

bb) Personenbezogene Daten dürfen nicht ohne Weiteres an Drittstaaten außerhalb der EU übermittelt werden. Dies ist gem. § 4b Abs. 2 und 3 BDSG nur dann zulässig, wenn in diesen Drittstaaten ein angemessenes Schutzniveau, das dem hei-

[19] Kritisch zur Auslegung des § 3 Abs. 8 BDSG, *Erd*, DuD 2010, 275 ff.

mischen vergleichbar ist, sichergestellt ist.[20] Bislang wurde dies z. B. für Kanada, Argentinien oder die Schweiz angenommen. Grundlage dieser von der EU-Kommission getroffenen Einschätzung[21] sind sowohl materielle als auch verfahrensrechtliche Kriterien.

Die Hürde des angemessenen Schutzniveaus kann – außerhalb der von der EU als Staaten mit angemessenem Datenschutzniveau festgelegten Staaten – auch dadurch überwunden werden, dass die in § 4c BDSG geregelten Ausnahmen gegeben sind.[22] Danach ist der Datenexport u. a. dann zulässig, wenn die empfangende Stelle im Ausland durch EU-Standardvertragsklauseln oder verbindliche Unternehmensregelungen ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gibt, § 4c Abs. 2 S. 1 BDSG.[23] Die Datenübermittlung ist dabei von der zuständigen Aufsichtsbehörde zu genehmigen, es sei denn, es werden die von der Europäischen Kommission veröffentlichten EU-Standardvertragsklauseln[24] unverändert verwendet.[25] Was die Datenübermittlung in die USA – welche als Land des „inadäquaten Datenschutzes" gelten[26] – betrifft, so ist anerkannt, dass das Datenschutzniveau dadurch gesichert werden kann, dass sich das entsprechende Unternehmen den sog. „Safe Harbor Principles" auf der Basis eines Abkommens zwischen dem amerikanischen Handelsministerium und der EU-Kommission unterwirft.[27]

Diese Safe-Harbor-Prinzipien und die damit verbundene Zertifizierung erwecken Vertrauen und sind damit einer der Garanten für Rechtssicherheit.[28] Gleichwohl werden sie in jüngster Zeit stark kritisiert.[29]

[20] *Schulz*, MMR 2010, 75 (78); *Pohle/Ammann*, CR 2009, 273 (277); *Gabel*, in: Taeger/ders. (Hrsg.), Kommentar zum BDSG, 2010, § 4b Rn. 10 ff.

[21] Vgl. Entscheidungen der Kommission zur Angemessenheit des Schutzes persönlicher Daten in Drittstaaten, http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_de.htm.

[22] Vertiefend zu den Ausnahmetatbeständen des § 4c BDSG: *Gabel*, in: Taeger/ders. (Hrsg.), Kommentar zum BDSG, 2010, § 4c Rn. 5 ff.

[23] *Hennrich/Maisch*, AnwZert ITR 15/2011, Anm. 2.

[24] Art. 26 Abs. 2, 4 RL 95/46/EG.

[25] *Reindl*, in: Taeger/Wiebe, Inside the Cloud – Neue Herausforderungen für das Informationsrecht, 2009, S. 447.

[26] *Spies*, MMR 2009, XI (XII).

[27] *Hennrich/Maisch*, AnwZert ITR 15/2011, Anm. 2; *Karger/Sarre* in: Taeger/Wiebe, Inside the Cloud – Neue Herausforderungen für das Informationsrecht, 2009, S. 435.

[28] Ausführlich *Hennrich/Maisch*, AnwZert ITR 15/2011, Anm. 2.

[29] Vgl. nur *Erd*, K&R 2010, 624 ff.; *Hennrich/Maisch* AnwZert ITR 15/2011, Anm. 2 m.w.N.

c) Gewährleistung von IT-Sicherheit (§ 9 S. 1 BDSG)

Gemäß § 9 S. 1 BDSG haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Hinsichtlich der automatisierten Verarbeitung oder Nutzung personenbezogener Daten wird die zentrale Datensicherheitsvorschrift des BDSG durch die Anlage zu § 9 S. 1 BDSG konkretisiert, welche – nicht abschließende – Maßnahmen enthält, die die Einhaltung der besonderen Anforderungen des Datenschutzes im Rahmen der innerbehördlichen Organisation sicherstellen sollen. § 11 BDSG stellt dabei auf klassische Datenverarbeitungsstrukturen ab. Seine Vorgaben eignen sich nur begrenzt für moderne und sich wandelnde Formen der Datenverarbeitung wie Cloud Computing.[30] Dies darf jedoch nicht zu einem Verzicht auf ausreichende Datensicherungsmaßnahmen führen.[31] Die vorzunehmenden Maßnahmen sollten nicht statisch, sondern vielmehr dynamisch geprüft und weiterentwickelt werden.[32]

3. Innovative Auslegung des BDSG

Die formaljuristische Betrachtung der datenschutzrechtlichen Vorschriften, wie sie in den Eckpunktepapieren der politischen Akteure, allen voran der Datenschutzbehörden zum Ausdruck kommt, ist allerdings nicht zwingend. Sie leidet vor allem unter einem erheblichen methodischen Mangel, weil sie zwingende Subsumtionsergebnisse auf Grundlage defizitärer Wertungsmaßstäbe ermittelt und damit mit mehreren Unbekannten rechnet.

So spricht § 11 Abs. 2 S. 1 BDSG davon, dass „der Auftragnehmer … unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen" ist. Hierbei werden wiederum die Maßnahmen und Maßgaben des § 11 Abs. 2 S. 2 BDSG als Minimum (!) zur Ausübung einer Datenherrschaft angesehen, die dem Auftraggeber als Ausdruck seiner Verantwortlichkeit im Sinne des § 11 Abs. 1 S. 1 BDSG verbleiben muss. Auf diese Weise entsteht durch die Forderung nach maximaler Datenherrschaft (§ 11 Abs. 1 S. 1 BDSG), maximaler Auswahlsorgfalt (§ 11 Abs. 2 S. 1 BDSG) und maximaler technisch-organisatorischer Vorkehrungen (§ 11 Abs. 2 S. 2 BDSG) ein quasi unerfüllbarer Anspruch gegenüber den Vertragspartnern im Cloud Computing. Weder kann der Auftraggeber die ihm zugedachte Rolle der Ausübung von Datenherrschaft noch der Auftragnehmer jene der Gewährleistung von Datensicherheit erfüllen.

Von mehreren „Unbekannten" ist hier deshalb zu sprechen, weil

[30] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 9 Rn. 30.

[31] Zur Erforderlichkeit der Datensicherungsmaßnahmen *Schultze-Melling*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 9 Rn. 19 ff.

[32] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 9 Rn. 30.

- die Herleitung von Datenherrschaft aus dem Prinzip der Verantwortlichkeit insofern willkürlich ist, da sie den Aspekt der notwendigen Verlagerung von Kompetenzen bei der Auftragsdatenverarbeitung übersieht.
- die Anforderungen an die „sorgfältige Auswahl" des Auftraggebers formuliert werden, ohne den Sorgfaltsmaßstab – auch unter Berücksichtigung der notwendigerweise fehlenden bzw. unzureichenden Expertise des Auftraggebers – zu ermitteln.
- die Eignung und Erforderlichkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit behauptet und zugrunde gelegt wird, ohne den Risikomaßstab zu diskutieren, der beim Cloud Computing als einem im Prinzip herkömmlichen Datenverarbeitungsvorgang auch wegen § 9 S. 2 BDSG (Erwägungen der Wirtschaftlichkeit) unter Beachtung der Verhältnismäßigkeit zu ermitteln ist.
- Kontrollrechte des Auftraggebers bis hin zu einer nachhaltigen Compliance-Kontrolle gefordert werden, ohne die Kontrolldichte zu ermitteln, die solche Maßnahmen erst verhältnismäßig und zumutbar erscheinen lassen.
- die Begründung von Unterauftragsverhältnissen unter Aspekten der Datenherrschaft in Frage gestellt wird und Weisungsbefugnisse des Auftraggebers in einem Umfang als zwingendes Recht gefordert werden, ohne die Autonomie des Cloud-Anbieters als beauftragtem Experten auch in Anbetracht unzureichender fachlicher Kompetenz des Auftraggebers zu berücksichtigen.

Die dem Cloud-Nutzer bei der Auftragsdatenverarbeitung obliegende Kontrolle der technischen und organisatorischen Maßnahmen nach § 11 Abs. 2 S. 2 Nr. 3, § 9 BDSG i.V.m. der Anlage zu § 9 BDSG sollte die Eigenheiten des Cloud Computing berücksichtigen. Eine enge und wortlautgetreue Auslegung des Begriffs „Festlegung der Maßnahmen" in § 11 Abs. 2 S. 2 Nr. 3 BDSG wird mit der Realität des Cloud Computing unvermeidlich kollidieren.[33] Diese Auslegung geht vom (bisher für den Bereich des Datenschutzes vorherrschenden) Fall der zentralen Datenverarbeitung aus und setzt damit in Inhalt und Reichweite eine Kontrollmöglichkeit des Auftraggebers voraus, welche sich beim Cloud Computing nicht durchhalten lassen wird. Bei territorial begrenzten Cloud-Diensten mag für den einzelnen Auftraggeber noch die Kontrolle jedes einzelnen Rechenzentrumsstandorts möglich erscheinen. Schon hier mutet dieser Aufwand aber nicht praxisgerecht an und kollidiert mit dem in § 9 S. 2 BDSG normierten Erforderlichkeitsgrundsatz. Je weiter die Diversifizierung der Cloud reicht, umso mehr wird zugleich der faktische Zugriff der datenverarbeitenden Stelle (Cloud-Nutzer) reduziert. In vielen Fällen – vor allem bei weltweit verteilten Standorten – stößt daher eine realistische Kontrollmöglichkeit aller in Betracht kommender Rechenzentrumsstandorte, die in Inhalt und Reichweite derjenigen bei zentraler Datenverarbeitung entspricht, an ihre Grenzen bzw. wird schlicht unmöglich.[34]

[33] So auch *Niemann/Hennrich*, CR 2010, 686 (690), die für eine dem technischen Fortschritt und der Realität des Cloud Computings angepasste, weite Auslegung plädieren.

Stimmt man allerdings einer teleologischen, an den Erfordernissen und Eigenheiten dezentraler Datenverarbeitungsprozesse orientierten Auslegung der „Festlegung der Maßnahmen" in § 11 Abs. 2 S. 2 Nr. 3 BDSG zu, kann auch bei Cloud Computing eine ausreichende Kontrollmöglichkeit des Auftraggebers vorliegen. Eine mögliche cloud-spezifische Lösung wird z. B. darin gesehen, dass die Kontrollpflichten des Auftraggebers bereits durch regelmäßige Prüfberichte des Auftragnehmers erfüllt werden können.[35] Im Rahmen standardisierter Leistungen für kleinere Unternehmen müsste der Auftraggeber seinen Kontrollpflichten zudem durch standardisierte Prüfberichte des Auftragnehmers nachkommen.

4. Fazit

Die skizzierten Beharrungstendenzen der Rechtsordnung – im Sinne eines formaljuristischen, unzeitgemäßen Festhaltens an überkommenen (weil technisch, wirtschaftlich oder gesellschaftlich überholten) Regulierungskonzepten – ist der erste „Sales Blocker" für die Verbreitung von Cloud-Computing-Angeboten, insbesondere solchen von global agierenden Anbietern. Dies ist aus Anbietersicht auch deshalb kritisch zu betrachten, weil die daraus resultierende Rechtsunsicherheit noch weitere potentielle Kunden abhalten wird, derartige Dienste in Anspruch zu nehmen.

Bei einer technisch-funktionalen Innovation wie dem Cloud Computing wird das Problem offensichtlich, dass das BDSG immer noch als Ausfluss des Volkszählungsurteils unter dem Aspekt des Persönlichkeitsschutzes ausgelegt wird. Und das, obwohl es im Jahr 2011 längst um professionelles Datenmanagement geht, welches im Rahmen einer (eigentlich durch § 9 S. 2 BDSG bereits angelegten) Wirtschaftlichkeitsbetrachtung nur durch ein Sicherheitskonzept reguliert werden kann, in das Kriterien eines sachadäquaten Risikomanagements einfließen.[36]

III. Pauschalisierungstendenzen im politischen Diskurs

Durch das hohe Abstraktionsniveau, in dem sich sowohl das „Cloud Computing" als Marketingbegriff als auch die darauf bezogenen politischen Aussagen bewegen, ergeben sich Chancen und Risiken für den Vertrieb entsprechender Produkte bzw.

[34] Vgl. auch *Niemann/Hennrich*, CR 2010, 686 (691).

[35] Vgl. *Niemann/Hennrich*, CR 2010, 686 (691) m.w.N.

[36] Die Politik interessiert in erster Linie nur, dass (!) bestimmte Technologien bzw. technologische Konzepte als „Innovation" gelten (sic!), weniger, was daran das Innovative ist. Vor allem aber scheut sich die Politik vor dem konsequenten Gedanken, dass Innovationen auch unvorhersehbare (!) Risiken mit sich bringen können. Es wäre eigentlich die Aufgabe der Politik, dies zu erklären, nicht aber, eine „Quadratur des Kreises" anzustreben, etwa im Sinne einer „sicheren Unsicherheit".

Dienstleistungen. Das spezifische Risiko besteht darin, dass pauschale Bedenken wie jene unzureichender Datensicherheit eine ganze Angebotspalette in Verruf bringen können, von der allenfalls bestimmte einzelne Dienste kritisch zu betrachten wären. Umgekehrt besteht für Cloud-Anbieter die Chance, das Profil ihrer Angebote in der Weise zu konkretisieren, dass die im politischen Raum formulierten rechtlichen und technischen Anforderungen erfüllt werden oder zumindest als erfüllbar erscheinen.

1. Wolkige Aussagen zum Cloud Computing

Analysiert man die zahlreichen Publikationen aus den Ministerien und anderen verantwortlichen Stellen, aus fachlichen Eckpunktepapieren und politischen Konzepten, so fällt auf, dass sämtliche Aussagen zum Cloud Computing auf einem sprachlich und inhaltlich signifikant hohen Abstraktionsniveau getroffen werden. Daraus ergeben sich spezifische Risiken für den Vertrieb von Cloud Services („Sales Blocker"). Allerdings bietet dieser Umstand auch Chancen.

a) Beispiel 1: Aktionsprogramm Cloud Computing des Bundeswirtschaftsministeriums

Das „Aktionsprogramm Cloud Computing" kann geradezu als kennzeichnend genannt werden für das hohe Abstraktionsniveau und die darin zum Ausdruck kommende Unverbindlichkeit der damit verbundenen politischen Aussagen.

So begrüßt der ehemalige Bundeswirtschaftsminister Brüderle „die gemeinsame Initiative von Wirtschaft, Wissenschaft und Politik, die Entwicklung, Verbreitung und Nutzung von Cloud Computing in Deutschland zu fördern."[37] Er spricht von „Zukunftschancen" und der Erschließung großer „Potenziale des Cloud Computings für den Wirtschaftsstandort Deutschland." Dies gelinge nur mit einer „Stärkung von Sicherheit und Vertrauen im Cloud Computing"[38], denn „vor allem kleinere Anwenderunternehmen, die nicht selbst aus dem IT-Bereich kommen", hätten noch „Hemmschwellen, Software oder Hardware in der „Wolke" des Internets zu nutzen." Sie würden sich fragen, „welchen Angeboten sie vertrauen und wohin sie Daten oder deren Verarbeitung sicher auslagern können. Ein kaum überschaubares Angebot, ständige Neuerungen, ungenügende Standardisierung und komplizierte Geschäftsmodelle erschwer(t)en oftmals die Entscheidungsfindung."

[37] Aktionsprogramm BMWi, Grußwort, S. 4 (auch folgende Zitate), http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

[38] In ähnlicher Weise nennt der ehemalige BITKOM-Präsident Scheer den Aspekt der Kostensenkung für Unternehmen, um zugleich die „hohen Anforderungen an Datenschutz, Informationssicherheit und Integrationsfähigkeit" zu betonen (Grußwort, S. 5). Auch der Präsident des CIOcolloquiums Endres greift hoch, wenn er von einer „zukunftsweisenden Technologie mit großem Entwicklungspotenzial" spricht. Voraussetzung hierfür sei aber wiederum die „Gewährleistung der Rechts- und Datensicherheit" (Grußwort, S. 6).

Deshalb solle der Technologiewettbewerb „Trusted Cloud" des Bundesministeriums für Wirtschaft und Technologie einen wichtigen Beitrag leisten, „Nutzbarkeit und Akzeptanz von Cloud-Technologien durch überzeugende Anwendungsbeispiele deutlich zu erhöhen." Bei Themen wie „Datenschutz, Interoperabilität und Sicherheit" sollen sich „traditionelle Standortstärken deutscher IT-Anbieter in die Entwicklung von Cloud Computing in Deutschland als Markenzeichen einbringen und so das Vertrauen in diese Technologie stärken."

Bereits in diesem Grußwort wird ein typisches Argumentationsschema deutlich:

Im ersten Schritt wird eine positive Grundhaltung erzeugt (Chancen und Potenziale). Diese Vorteile erfordern, so der zweite Schritt, Sicherheit und Vertrauen, also Attribute, deren Berechtigung wohl niemand in Zweifel ziehen kann. Ähnlich pauschal werden im dritten Schritt Risiken (zum Beispiel ungenügende Standardisierung oder komplizierte Geschäftsmodelle) benannt, die für sich sprechen sollen und deshalb jeder empirischen Beweiswürdigung entzogen werden. Besonders problematisch ist schließlich der vierte Schritt, wonach wiederum eine Lösung auf der Grundlage der im zweiten Schritt konstatierten Grundbedingung („Sicherheit und Vertrauen") so ins Spiel gebracht wird, dass Alternativen entbehrlich erscheinen. Wenn dort nämlich von den „traditionellen Standortstärken deutscher Anbieter" im Sinne der Marke „made in Germany" die Rede ist[39], werden bestimmte Geschäftsmodelle mit der Erfüllung abstrakter Anforderungen gleichgesetzt, was weder in der Sache zwingend noch vor dem Hintergrund einer Diskriminierung ausländischer Anbieter gerechtfertigt ist.

b) Beispiel 2: BSI-Eckpunktepapier 2011

Das signifikant hohe Abstraktionsniveau im politischen Diskurs zeigt sich freilich nicht nur auf der politischen, sondern auch auf der fachlichen Ebene. Beispielhaft seien hierfür Passagen aus dem Eckpunktepapier des BSI[40] genannt.

> „Obwohl weltweit IT-Dienstleistungen aus der „Wolke" immer stärker in Anspruch genommen werden, zeigen fast alle Umfragen und Studien, dass es auch eine Vielzahl von Bedenken gibt, die Anwender vor der Nutzung von Cloud Computing Diensten zurückschrecken lassen. Als eines der größten Hindernisse wird immer wieder mangelndes Vertrauen in die Sicherheit der bereitgestellten Services genannt. Als zentrale Stelle des Bundes für die In-

[39] Aktionsprogramm BMWi S. 19: „Besonders wichtige Alleinstellungsmerkmale des deutschen IT-Sektors sind dabei Zuverlässigkeit, Sicherheit und Datenschutzkonformität der angebotenen Cloud-Lösungen", http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

[40] Siehe BSI, Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf;jsessionid=32FD3C8BD85C0219423B90660EC5A4DD.2_cid286?__blob=publicationFile.

formationssicherheit ist es dem BSI wichtig, die Aufbauphase von Cloud Services aktiv mitzugestalten."[41]

„Aufgrund der erwarteten technischen und wirtschaftlichen Potenziale wird sich Cloud Computing voraussichtlich am Markt durchsetzen können, allerdings nur, wenn die Anbieter es schaffen, die Fragen der Kunden zur Informationssicherheit und zum Datenschutz zu klären. Mit zunehmender Verbreitung in der Fläche werden allerdings Cloud Computing Angebote für Angreifer attraktiver, auch aufgrund der Konzentration vieler geschäftskritischer Ressourcen in zentralen Rechenzentren sowie der erforderlichen Standardisierung der Komponenten und Schnittstellen. Daher wird es auf lange Sicht nötig sein, internationale Standards für Informationssicherheit zu erarbeiten und zu etablieren, auf deren Grundlage Plattformen für das Cloud Computing überprüft und zertifiziert werden können. Eine der zentralen Aufgaben in den nächsten Jahren wird es daher sein, internationale Standards für die Informationssicherheit im Bereich Cloud Computing zu erarbeiten und zu etablieren, auf deren Basis die Sicherheit von Cloud Computing Anbietern zertifiziert werden kann. Nur durch international anerkannte Zertifizierungen von Cloud Computing Anbietern bzw. deren Services wird ein ausreichendes Vertrauen auf Seiten der Kunden geschaffen werden können."[42]

2. Spezifische Risiken der Pauschalisierung und Abstrahierung

Pauschalurteile, wie man sie im Hinblick auf die (gerade auch rechtliche) Beurteilung des Cloud Computing häufig vorfindet, können zum „Sales Blocker" avancieren. Störungen des Vertriebs entsprechender Angebote sind in zweifacher Weise denkbar:

Zum einen nimmt eine pauschale Distanzierung zu „Cloud Computing" (etwa durch Datenschützer) den Anbietern die Chance, die Angemessenheit und Rechtskonformität des eigenen Angebots werbend nach außen zu tragen. Insoweit muss auch die subtile Wirkung von Aussagen wie „mangelndes Vertrauen in Sicherheit und Datenschutz" berücksichtigt werden. Derartige Äußerungen rücken Cloud Computing in das Licht von etwas „Verbotenem" oder „Unzulässigem". Ebenso wenig werden die einzelnen Angebote eines „Cloud Computing" näher spezifiziert (meist bleibt sogar gänzlich unerwähnt, welche Differenzierungen es überhaupt gibt) bzw. wird bei den Bedenken im Hinblick auf Datenschutz, Datensicherheit und Vertrauen nicht näher unterschieden, welche Daten auf welche Weise überhaupt gefährdet sind. Auf diese Weise erscheint der „Datenschutz" für das „Cloud Computing" wie ein Angst verbreitendes Schreckgespenst, dessen konturenlosen Gefahren kaum entgegengetreten werden kann.

Zum anderen verhindert die Abstrahierung der Aussagen zu „Cloud Computing und Compliance" im politischen Diskurs, dass Unternehmen sich auf richtungsweisende Entscheidungen der Regierung bzw. des Parlamentes einstellen und ihre Geschäftsmodelle auf entsprechende Weichenstellungen abstimmen können. Die politischen Entscheidungsträger scheuen jedwede Festlegung und überlassen das Feld damit jenen Instanzen, die sich aus heterogenen Motiven vereinzelter „Mutiger" positionieren, wie etwa den Datenschutzbehörden.[43] Diese Instanzen aus dem Verwaltungsvollzug sind aber nicht unmittelbar demokratisch legitimiert. Somit kann ihre Haltung nicht als Handlungsmaßstab dienen.

[41] Aktionsprogramm BMWi, S. 8, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

[42] Aktionsprogramm BMWi, S. 68.

3. Chancen der Pauschalisierung und Abstrahierung

Wie bereits aufgezeigt bergen pauschale Urteile und stark abstrahierende politische Aussagen zu technischen Innovationen Risiken für die Etablierung von Geschäftsmodellen, die auf eine verlässliche politische Weichenstellung angewiesen sind. Unternehmen, die auf diese Weise verunsichert werden, können von diesen Umständen aber auch profitieren:

Ihnen bietet sich die Chance, das Profil ihrer Angebote in einer Weise zu konkretisieren, dass die im politischen Raum formulierten rechtlichen und technischen Anforderungen erfüllt werden oder zumindest als erfüllbar erscheinen. Im Grunde genommen geht es hier wie da um die normative Kraft des Faktischen:[44] Unternehmerisches Marketing trifft auf politisches Marketing. Innovative Produkte und Dienstleistungen werden in ihren Compliance-Anforderungen auf jener Abstraktionshöhe als rechtskonform dargestellt, die die Politik in ihren Aussagen „eingestellt" hat. Man greift also die politisch formulierten Ansprüche in ihrer pauschalen und abstrakten Form auf und subsumiert das eigene Datenschutzkonzept darunter. Das fällt aufgrund des hohen Abstraktionsgrades nicht schwer. Die unternehmerische Chance liegt hier in der Deutungshoheit: Wann genau ist ein Cloud-Computing-Dienst rechtskonform? Soweit dies nicht in verbindliche Regeln gefasst ist, können eigene Konzepte kaum widerlegt werden.

Denkbar ist, dass genau diese Vorgehensweise die Politik veranlasst, „nachzulegen". Dies kann in einem Dialog zwischen Politik und Unternehmen münden, der zur Konkretisierung bisheriger bloß formulierter Ansprüche führt. Diese „dialogische Konkretisierung" trägt dazu bei, die als „Sales Blocker" angeführte Rechtsunsicherheit zu beseitigen.

4. Fazit

Neben den Beharrungstendenzen der Rechtsordnung de lege lata (oben II.) erweisen sich die Pauschalisierungs- und Abstrahierungstendenzen de lege ferenda im politischen Diskurs als weiterer „Sales Blocker", soweit dadurch verhindert wird, not-

[43] Beispielhaft vgl. *Weichert*, DuD 2010, 679 ff.

[44] Darauf stellt im Ergebnis auch Roger Albrecht in einem Artikel vom 19. Mai 2011 ab: http://www.enterprisecioforum.com/de/article/cloud-computing---daran-führt-kein-weg-vorbei.

wendige Schutzmechanismen zum Ausgleich divergierender Interessen nach verlässlichen Vorgaben in die angebotenen Produkte und Dienstleistungen zu integrieren.

Ergreifen Anbieter innovativer Dienste jedoch die Chance, Deutungshoheit und Konkretisierungsmacht bei der Formulierung der Compliance-Anforderungen zu übernehmen, dann avanciert das Zögern und Zaudern der politischen Entscheidungsträger möglicherweise zum „Enabler" solcher Innovationen. Für die Etablierung von Angeboten am Markt genügt es dann nämlich, eine Rechtskonformität ohne plausiblen Widerstand zu behaupten.

IV. Abschottungstendenzen der Wirtschaftsordnung

Beim Cloud Computing zeigt sich in besonders starker Weise für außereuropäische Anbieter das Problem, dass industriepolitische Präferenzen durch rechtliche Bedenken verbrämt werden. Signifikanter Ausdruck dessen ist die „Cloud made in Germany".

1. IT-Politik als Industriepolitik

Wenn man die „Sales Blocker" ermitteln will, die den Cloud-Computing-Anbietern in den nächsten Jahren den Vertrieb ihrer Produkte und Dienstleistungen erschweren könnten, ist neben den rechtsdogmatischen und rechtspolitischen Hürden auch zu bedenken, dass Cloud Computing innerhalb der IT-Innovationen geradezu paradigmatisch für „grenzüberschreitende Angebote" steht und damit eine natürliche Affinität zum Weltmarkt aufweist. Solche Globalisierungstendenzen werden regelmäßig durch Abschottungstendenzen der Wirtschaftsordnung beantwortet: IT-Politik ist Industriepolitik. Selbst wenn es eindeutige Regeln zur Datenverarbeitung in Cloud-Umgebungen gäbe und keine politischen Vorbehalte oder Verzögerungen vorhanden wären, wäre der globale Wettbewerb um die besten Angebote trotzdem nur bedingt eröffnet. So paradox es auch erscheinen mag: Gerade die vielfach attestierte hohe Attraktivität der Cloud Services verhindert den Eintritt in nationale Märkte, weil diese sich gegen internationale Konkurrenz abzuschotten versuchen.

In diesem Sinne forderte etwa Harald Lemke 2005, seinerzeit noch CIO des Landes Hessen, eine „knallharte IT-Industriepolitik":[45] „Wenn wir unsere Produkte in aller Welt verkaufen wollen, müssen wir auch der Showcase für diese Innovationen sein."[46]

2. „Cloud made in Germany"

Und so werden die bereits vorstehend im Rahmen des politischen Diskurses zitierten Vorbehalte im Sinne von Datenschutz und Datensicherheit strategisch zur

[45] http://www.gfaller.de/index.php?id=117.

[46] http://www.gfaller.de/index.php?id=117.

Stärkung der eigenen Produkte verwendet. Sehr deutlich wurde dies auf der Cloud Computing Conference, die am 6. Oktober 2010 auf Einladung des BITKOM in Köln durchgeführt wurde.[47]

Dort ging es – schon wegen der Keynotes von Microsoft-Chef Steve Ballmer und Werner Vogels, CTO Amazon – zunächst um die internationale Dimension des Cloud Computing und dessen revolutionäre Kraft: „Die Cloud verändert alles." Weil allerdings die „Vertrauensfrage" buchstäblich im Raum stand und es bei allen Visionen doch galt, der permanenten Datenschutz-Kritik zu begegnen, tat sich Telekom-Chef Obermann sehr leicht, beides vermeintlich in Einklang zu bringen. Vor allem Firmen, die geschäftskritische Anwendungen aus der Cloud beziehen wollen, verlangten nach Rechtssicherheit und garantierten Standards für Qualität und Stabilität, so Obermann. Das gelte gerade für die Datensicherheit. Deshalb seien die strengen deutschen Bestimmungen zum Datenschutz ein Standortvorteil für die „Cloud Made in Germany".[48]

Natürlich mag diese Deutung auslegungsfähig sein.[49] Es ist aber bezeichnend, dass ausgerechnet die vermeintlichen „Sales Blocker" der „strengen Bestimmungen zum Datenschutz" zum „Verkaufsschlager" verkehrt werden. Wenngleich der Gedanke vom „Datenschutz als Geschäftsmodell" einer gängigen Denkweise im Datenschutzrecht entspricht[50], geht es aus Sicht eines deutschen Unternehmens doch eher um eine Abschottungsstrategie, wie dies etwa auf dem Markt sozialer Netzwerke schon länger von Unternehmen wie XING oder der VZ-Gruppe gegenüber dem amerikanischen Marktführer Facebook gepflegt wird.[51]

3. Fazit

IT – zumal in einem globalen Markt – ist ein Milliardengeschäft. Eine Innovation wie Cloud Computing beflügelt Märkte und verheißt insbesondere durch die immanenten Skalierungsmöglichkeiten eine hohe Marktdurchdringung. Dies macht Cloud Computing zu einem volkswirtschaftlichen Faktor von unschätzbarer Größe. Dass dies aus Sicht nationaler Staaten industriepolitische Implikationen mit sich bringt, ist nicht näher erläuterungsbedürftig. So mag eine im Aufbau begriffene Marke „Cloud made in Germany" nicht mehr als eine Fußnote in der weltweiten Compliance-Diskussion sein. Der darin sichtbare Trend zur Abschottung nationaler bzw. re-

[47] Auf dieser Konferenz referierte der Verfasser dieser Studie zu „Cloud Computing zwischen Verantwortung und Vertrauen", hierzu http://www.cloud-practice.de/news/cloud-computing-zwischen-vertrauen-und-verantwortung. Hierzu auch http://www.welt.de/print/welt_kompakt/webwelt/article10147880/Revolution-aus-den-Wolken.html.

[48] http://www.telekom.com/dtag/cms/content/dt/de/931006?printversion=true.

[49] Differenzierend im Sinne einer Standortunabhängigkeit *Heckmann*, LTO v. 15.11.2010, http://www.lto.de/de/html/nachrichten/1929/cloud-made-in-germany-als-vertrauensgarant/ .

[50] Vgl. *Assion*, Telemedicus v. 01.04.2010, http://www.telemedicus.info/article/1691-Das-Zeitalter-des-Datenschutzes-keinesfalls-vorbei.html.

[51] Siehe zum Datenschutz in sozialen Netzwerken *Erd*, NVwZ 2011, 19 ff.

gionaler Märkte ist unterdessen ein „Sales Blocker" jedenfalls für solche Dienste, die, wie das Cloud Computing, ihren entscheidenden Effekt gerade in der grenzüberschreitenden Datenverarbeitung haben. Diese Hürde ist auch deshalb ernst zu nehmen, weil bestimmte Geschäftsmodelle nicht ihrer Konkurrenz willen, sondern aus vordergründigen Compliance-Erwägungen diskreditiert werden können.

V. Ideologisierungstendenzen der fachlichen Ebene

Für Cloud Dienste besteht ein erhöhtes Risiko einer „kalten Enteignung" durch Standardisierung. Cloud Computing zeichnet sich durch eine hohe Skalierbarkeit (insbesondere durch Anpassung an unterschiedliche Bedarfe) und die damit einhergehende Innovationsoffenheit aus. Besonders autoritativ gesetzte (staatliche) Standards wirken als Störfaktor, unabhängig davon, ob sie bewusst oder unbewusst gegen bestimmte Erscheinungsformen des Cloud Computing gerichtet sind.

1. Standardisierung als erwartungssteigernde „Zauberformel"

„Standardisierung" zählt zu jenen technisch-organisatorischen Vorkehrungen in heterogenen (IT-) Systemen, deren Begrifflichkeit durchweg positiv besetzt ist. Sie gelten als erstrebenswert und nützlich und dienen geradezu als „Zauberformel", die Funktionsfähigkeit von Systemen (wieder-)herzustellen. Wesentliche Wachstums- und Servicepotentiale lassen sich durch eine Abstimmung von Standards und Interoperabilität erreichen.[52] So übernimmt auch die Politik gerne Forderungen nach (IT-) Standardisierung in ihr Regulierungskonzept, um (vermeintliche) Missstände durch „Lösungen am Reißbrett" zu beseitigen. Begriffe wie „Standard" und „Interoperabilität" werden immer häufiger genannt und finden zunehmend Eingang in die Gesetzessprache.[53] Ein Beispiel für die rechtlich durchaus bedenkliche IT-Standardisierung im öffentlichen Sektor bietet SAGA.[54]

So plausibel die Forderung nach Standardisierung oft klingt (und zuweilen auch tatsächlich berechtigt ist), führt sie doch zu Problemen, die von der Rechtswissenschaft bislang kaum beachtet wurden. Dies liegt daran, dass sowohl der Begriff des „Standards", insbesondere jener des IT-Standards, als auch seine rechtliche Einordnung und (Eingriffs-)Wirkung ungeklärt sind.

Obwohl es bereits seit vielen Jahrzehnten Standardisierungsverfahren und -gremien auf nationaler und internationaler Ebene gibt, existiert bis heute kein anerkannter bzw. einheitlich gebrauchter Rechtsbegriff des Standards.[55] Dies liegt nicht zuletzt daran, dass „Standard" sowohl im Kontext von Normen als auch im Zusammenhang mit Qualitätsmerkmalen verwendet wird. Bezogen auf Informationstechnik wird Standard[56] zuweilen auch mit Interoperabilität[57] gleichgesetzt oder verwechselt. Im Rahmen einer noch auszubildenden „Rechtstheorie der Standardisierung" sollte unterschieden werden: Was sind Standards (Produktstandards, Verfahrensstandards, normierte Formate und Spezifikationen), wer ist zur Festlegung solcher Standards berufen und was soll mit dem Setzen von Standards rechtlich bewirkt werden?

Diese Begriffs- und Abgrenzungsschwierigkeiten werden noch verstärkt, wenn man den Begriff „Interoperabilitätsstandard" hinzunimmt: Zum Teil wird dieser Begriff für Softwarestandards verwendet, die aufgrund ihrer technischen Eigenheiten, einer etwaigen Lizenzfreiheit („offene Standards") oder anderer Vertriebs- und Einsatzbedingungen ein besonderes Maß an Interoperabilität in einer vorgegebenen IT-Umgebung gewährleisten. Genau genommen ist ein solcher Begriff entbehrlich, zumindest aber irreführend. Denn im Prinzip sorgt jeder Standard für Interoperabilität bezüglich jener IT-Komponenten, deren Verknüpfung sich an genau diesem Standard orientiert.[58]

Wenn man den Begriff „Interoperabilitätsstandard" (IO-Standard) jedoch nicht in dieser redundanten Weise verwenden will, darf man ihn nicht als „Interoperabilität von Standards" oder „Interoperabilität durch Standards" verstehen, sondern im Sinne einer Standardisierung von Interoperabilität. Dann aber geht es um Standards im Sinne von Regeln (Normen), deren Einhaltung Interoperabilität (hier: das funktionale Zusammenwirken von Informationssystemen zum unmittelbaren Datenaustausch) sicherstellt. Das können technische oder Verfahrensstandards sein. Als technische

[52] Vgl. *Kühn/Riedl/Spichiger,* in: Schweighofer, Semantisches Web und Soziale Netzwerke im Recht, 2010, S. 131 ff.

[53] Vgl. Art. 91c GG „Standards", § 2 BSI-Gesetz „Sicherheitsstandards"; § 2 EGovG Schleswig-Holstein.

[54] Hierzu aus verfassungsrechtlicher Sicht grundlegend *Heckmann,* CR 2006, 1 ff.

[55] U.a. zum Begriff „Standard" im allgemeinen Verständnis *Steinmetz,* IT-Standardisierung und Grundgesetz, 2010, S. 25 ff.

[56] Von einem Standard kann man (allgemein) sprechen bei einer „Vereinbarung, welche für die Nutznießer eines Objekts in Bezug auf bestimmte Eigenschaften dieses Objekts von einer anerkannten Stelle als verbindlich getroffen wird". Eine gesetzliche Definition von Standards findet sich nunmehr in § 2 Nr. 2 des E-Government-Gesetzes Schleswig-Holstein: „Im Sinne dieses Gesetzes sind Standards technische und prozessuale Standards. Ein technischer Standard ist die Festlegung einer technischen Vorgehensweise auf einem bestimmten Gebiet. Hierzu zählen insbesondere die Definition von Schnittstellen, die Festlegung von Datenschemata und von Daten- und Dateiformaten für die Speicherung, den Austausch sowie für die Be- und Verarbeitung von Daten. Ein prozessualer Standard ist die Festlegung von organisatorischen Bedingungen oder der Vorgehensweise hinsichtlich des Verfahrens auf einem bestimmten Gebiet. Hierzu zählt insbesondere die Festlegung von zeitlichen und fachlichen Prozessschnittstellen."

[57] Interoperabilität (für sich) ist die Eigenschaft eines heterogenen Systems, dessen Komponenten funktional zusammenwirken zu lassen.

[58] In diesem Sinne konnte man den Standard für Videokassetten VHS auch als Interoperabilitätsstandard bezeichnen, weil er nämlich die Interoperabilität dieser Videokassetten mit VHS-Videorekordern gewährleistete. In ähnlicher Weise wird der Softwarestandard ODF auch als Interoperabilitätsstandard gehandelt, weil seine Verwendung Interoperabilität von Office Dokumenten verspricht.

Spezifikation kommen besonders die Definition von Schnittstellen und die Festlegung einheitlicher Übertragungsprotokolle oder Konvertierungsprogramme in Betracht. Die Festlegung derartiger IO-Standards ist ein Signal an den Markt, die Weiterverwendungsmöglichkeiten von Informationen durch Schaffung technischer Übergänge zu erweitern, d. h. die (latente) Abschottungswirkung „proprietärer" Systeme zu vermeiden oder zu überwinden. In einem Satz: Ein IO-Standard beschreibt die Normierung von Übergängen in einem heterogenen System.

Die politische (und auch administrative) Forderung einer IT-Standardisierung weckt Erwartungen, die kaum erfüllbar sind. Komplexe heterogene IT-Systeme sind durch IT-Standards nur bedingt regulierbar. Vor allem können autoritativ (extern) gesetzte IT-Standards wie ein Fremdkörper wirken, der zu unerwünschten Anpassungen und Veränderungen des regulierten IT-Systems führt, ohne dass dies durch die erstrebten Schutzwirkungen zwingend veranlasst wäre.

2. Risiken einer unbedachten Standardisierung von Cloud-Technologien

Unnötige oder sachfremd motivierte IT-Standards wirken sich in zweifacher Hinsicht negativ auf den Vertrieb aus:

Zum einen haben es Cloud-Anbieter, deren Angebote in einem oder mehreren Punkten nicht standardkonform erscheinen, schwer, sich gegenüber Konkurrenzangeboten zu behaupten, die ihrerseits mit ihrer Standardkonformität werben werden.

Zum anderen führen diffuse IT-Standards (soweit diese nicht „Gesetzeskraft" haben) zu einer Verunsicherung der Entwicklungsabteilungen auf Anbieterseite, weil unklar bleibt, welchen Verbindlichkeitsgrad und welche „Halbwertszeit" diese Cloud-Standards haben.

Weiter können Risiken auch dahingehend bestehen, dass ein marktführender „Player" Leistungen nach seinen Vorstellungen standardisiert und andere Unternehmen aufgrund der Marktdominanz dazu zwingt, diesen Standard auch zu akzeptieren. Cloud-spezifisch kann auf die Gefahr eines „Vendor-Lock-Ins" verwiesen werden, also einer Herstellerabhängigkeit: Leistungen sind so spezifisch konfiguriert, dass ein Wechsel nur mit großem Aufwand durchführbar wäre.

3. Fazit

Cloudbezogene IT-Standards wirken sich mittelbar auf die Verwirklichung von Cloud-Computing-Geschäftsmodellen aus. Sie haben – anders als gesetzliche Datenschutzbestimmungen – keine unmittelbare Verbots- oder Gebotswirkung. Vielmehr wirken sie im Regelfall wie eine Empfehlung an die Kunden, (nur) standardkonforme Angebote in Anspruch zu nehmen.

Allerdings ist auch eine solch bloße Empfehlung nicht frei von rechtlichen Voraussetzungen. So kann IT-Standardisierung in Konflikt mit Verfassungs- und Vergaberecht geraten:[59] IT-Standards haben eine erhebliche marktregulierende Wirkung, indem sie all jene IT-Produkte und Dienstleistungen vom Beschaffungsmarkt, insbesondere jenem der öffentlichen Hand, abkoppeln, die sich als nicht „standardkonform" erweisen. Damit wird die unter Bedarfsgesichtspunkten notwendige Interoperabilität ohne Not durch einen Standardisierungsprozess gesteuert, der zudem mangels kohärenter Delegations- und Entscheidungsstrukturen intransparent bleibt. Der damit einhergehende faktische Grundrechtseingriff zu Lasten der verdrängten Marktteilnehmer bedarf der verfassungsrechtlichen Rechtfertigung. Diese scheitert bereits am Fehlen einer gesetzlichen Grundlage für marktorientierte Technologievorgaben behördlicher Standardisierungsstellen.

Die Empfehlung an die Kunden, (nur) standardkonforme Angebote in Anspruch zu nehmen, kann sich negativ auf Cloud-Angebote auswirken. Gerade weil die Forderung nach „Standardisierung" positiv besetzt ist (die Marktteilnehmer assoziieren damit vielfach technisch notwendige Interoperabilität), wird ein – möglicherweise sachlich nicht gerechtfertigtes – Vertrauen in diese Standards gesetzt, was gerade vor dem Hintergrund der Datenschutzdiskussion beim Cloud Computing Kaufentscheidungen beeinflussen kann.

Umgekehrt ist aber auch zu betonen, dass Cloud Computing in einem bestimmten Umfang Standards braucht. Es kommt nur darauf an, wer diese setzt bzw. in welchem Verfahren diese zustande kommen (autoritativ oder marktorientiert). Der „Sales Blocker" ist deshalb nicht die Cloud-Standardisierung als solche, sondern sind gewisse Ideologisierungstendenzen bei dieser Standardisierung. Ähnlich wie dies schon bei der Open-Source-Debatte[60] und bei SAGA (.NET vs. J2EE)[61] zu beobachten war, ist das Risiko gegeben, dass Entscheidungsträger aus einer intransparenten und rechtlich schwer begründbaren Haltung heraus bestimmte Hersteller, ihre Produkte oder Geschäftsmodelle kritisieren und – eine offene Abwägung scheuend – das gewünschte Ergebnis in die Form „passender" Standards kleiden. Dem müsste entgegengewirkt werden.

VI. Destabilisierungstendenzen des Cloud Marketing

Der Erfolg von „Cloud Computing" steht und fällt mit der Gewinnung des Vertrauens der Marktteilnehmer. Vertrauensverlust ist der definitive „Sales Blocker", Vertrauensstiftung dementsprechend der wesentliche Erfolgsfaktor. Aus Anbietersicht kommt es darauf an, die Definitionshoheit über die Vertrauenserwartungen zu erhalten.

---

[59] Hierzu näher *Heckmann*, CR 2006, 1 ff.
[60] Hierzu *Heckmann*, CR 2004, 401 ff.
[61] Hierzu *Heckmann*, CR 2006, 1 ff.

1. Vertrauensverlust und Vertrauensvorschuss beim Cloud Computing

Wenn es ein Wort gibt, das im Kontext der IT-Entwicklung in letzter Zeit geradezu inflationär gebraucht wird, dann ist es „Vertrauen", das in diesem Kontext gar als Zauberwort[62] bezeichnet wird. Je nach Standpunkt und Intention geht es einmal um das fehlende und einmal um das notwendige Vertrauen in Cloud-Angebote.

Im Prinzip spitzt sich die gesamte Diskussion um Cloud Computing auf die „Vertrauensfrage" zu:

So bringt beispielsweise Katja Friedrich in ihrem Blogeintrag vom 30. 6. 2011[63] die Debatte auf den Punkt:

> „Cloud dreht sich nicht mehr nur um Infrastruktur und Software, sondern vielmehr um Mehrwerte, die über ein Cloud-Angebot geschaffen werden müssen. Laut Gartner wird sich der Nutzen eines Cloud-Angebotes von „Capacity on demand" zu „Capability on demand" verschieben. Wir schließen uns dieser Einschätzung an. Im Umkehrschluss bedeutet das für Unternehmen, dass sie einem Cloud-Partner großes Vertrauen entgegen bringen müssen. Vertrauen ist im Moment aber noch ein Hindernis für klassische Off-shoring-Cloudanbieter in Deutschland. In Synergie jedoch können deutsche und indische Cloud-Anbieter und IT-Dienstleister die Vertrauensfrage lösen. …
>
> Security, Safety, Privacy – diese Schlagworte sind nach wie vor große Herausforderungen beim Thema Cloud. Diese Überlegungen sind bei weitem nicht mehr theoretischer Natur, …. Auch hier gilt für Unternehmen: Vertrauen wird der Schlüssel sein müssen. Hundertprozentige Sicherheit gibt es nicht, aber vertrauenswürdige Partner."

Und die PWC-Studie „Cloud Computing im Mittelstand" formuliert:

> „Anbieter sollten daher alle zur Verfügung stehenden Zertifizierungen und Nachweise unabhängiger Dritter nutzen, um das zu tun, was offenkundig am meisten fehlt: Vertrauen schaffen."[64]

In der Studie „XaaS Check 2010 – Status Quo und Trends im Cloud Computing" kommen die Autoren der TU Darmstadt, IT Research und Wolfgang Martin Team zum Fazit:

> „Hindernisse für die Nutzung von Cloud Computing sind und bleiben die Themen Sicherheit, Vertraulichkeit, rechtliche Aspekte sowie Compliance-Anforderungen."[65]

[62] http://www.ishpc.de/2011/05/31/zauberwort-vertrauen-die-cloud-im-mittelstand/.

[63] http://www.cirquent-blog.de/2011/06/30/cloud-was-zahlt-sind-vertrauen-und-mehr wert/.

[64] http://www.pwc.de/de_DE/de/mittelstand/assets/Cloud_Computing_Mittelstand.pdf, Studie S. 33.

[65] http://www.xaas-check.eu/download.php?cat=00_Willkommen&file=2010-XaaS-Check-Report.pdf.

So resümiert auch Dr. Guido Möllering, Max-Planck-Institut für Gesellschaftsforschung, Köln, in seiner Untersuchung über Cloud Computing aus der Sicht der Vertrauensforschung[66] unter der Überschrift „Verantwortung zeigen":

> „So wird es auch im Cloud Computing über alle Bemühungen um fehlerfreie Technologien, lückenlose Rechtsapparate, konsequente Aufsichtsinstanzen und vorsorgliche Versicherungen hinaus immer nötig sein, dass die Beteiligten signalisieren, dass sie Verantwortung für das System tragen wollen – auch über ihre individuellen Verpflichtungen hinaus. Geschieht dies, werden sich viele weitere Akteure in die Wolke hineinwagen. Ich habe in meinem Vortrag herausgestellt, dass es in der Internet Cloud vor allem auf generalisiertes Vertrauen und Vertrauen in abstrakte Systeme ankommt. Wo technische Sicherungsmechanismen an Grenzen stoßen, müssen die verbleibenden Lücken durch soziale Mechanismen geschlossen werden. Daher gilt es, Gelegenheiten zu schaffen und zu nutzen, bei denen die das System tragenden Akteure in Erscheinung treten, ihre Verantwortungsbereitschaft beweisen und auch gegen die vorgehen, die verantwortungslos handeln – egal, ob diese auf der Seite der Anbieter, der Nachfrager oder der Behörden stehen. Es geht nicht um absolute Sicherheit, sondern um den guten Willen. Der allein reicht wiederum auch nicht aus – das wäre ja weltfremd – aber er muss stets erkennbar sein, wenn Cloud Computing mit Vertrauen effizienter oder überhaupt erst in der Breite möglich werden soll."

Auch auf der Cebit 2011, die Cloud Computing als herausragendes Thema platzierte, wurden Vertrauensdefizite hervorgehoben.[67]

2. Definitionshoheit über die Vertrauenserwartungen

Vertrauen hängt mit Erwartungen zusammen.[68] Wenn etwa Cloud-Kunden den Diensten und Services ihrer Anbieter Vertrauen schenken, dann verknüpfen sie damit eine bestimmte Erwartung, etwa im Hinblick auf deren fachliche Kompetenz oder dahingehend, wie ihr Vertragspartner mit ihren Daten und den damit verbundenen Interessen (im Krisenfall) umgeht.[69] Wer wiederum bestimmten Anbietern oder Angeboten misstraut, drückt damit auch eine (negative) Erwartung aus, nämlich dass jene Akteure die (vielleicht hochgesteckten) Anforderungen an die Verfügbarkeit, Vertraulichkeit oder Integrität der ausgelagerten Daten nicht erfüllen.

Wenn Vertrauen also der wesentliche (Miss-) Erfolgsfaktor für Cloud Computing ist und die Investition von Vertrauen im Wesentlichen mit der Erfüllbarkeit von Vertrauenserwartungen zusammenhängt, ist es für einen Anbieter von entscheidender Bedeutung, die Definitionshoheit über diese Vertrauenserwartungen nicht zu verlieren. Welche Erwartungen bzw. Anforderungen an Cloud-Computing-Dienste gestellt werden, hängt auch damit zusammen, wie der Anbieter den Inhalt seines Angebots,

[66] http://www.mpifg.de/people/gm/downloads/MK_Moellering_VernebeltesVertrauen_Dokumentation_100209.pdf.

[67] http://www.welt.de/wirtschaft/webwelt/article12660443/Auf-der-Cebit-kaempfen-die-Konzerne-um-Vertrauen.html.

[68] *Luhmann*, Vertrauen, 4. Aufl. 2000, S. 103 ff.

[69] Zu Vertrauen in virtuellen Räumen, *Heckmann*, K&R 2010, 1 ff.

die eigene Kompetenz zu dessen Erfüllung und den Umgang mit verbleibenden Risiken kommuniziert. Hier wird es besonders darauf ankommen, keine übertriebenen und damit praktisch unerfüllbaren Erwartungen aufkommen zu lassen. So ist es eine große Herausforderung an das Cloud Marketing, die Vorzüge, den Mehrwert und damit verbundene Leistungsversprechen zu verbreiten, ohne die jeweiligen Risiken und Einschränkungen im Portfolio zu verschweigen.

3. Fazit

Die Diskussion um fehlendes Vertrauen, Vertrauensdefizite oder Misstrauen in Cloud Computing erweist sich als wesentlicher „Sales Blocker". Man kann insoweit von Destabilisierungstendenzen sprechen. Innovationen haben es per definitionem ohnehin schwer, Vorbehalte gegenüber dem Neuen, dem Unbekannten, dem Riskanten auszuräumen. Das wird noch gesteigert, wenn solche Vorbehalte mit einem diffusen, generalisierenden „Misstrauen" gegenüber Geschäftsmodellen begründet werden, die bestimmte Risiken implizieren und diese über einen dezidierten Mehrwert der Transaktion zum Ausgleich bringen.[70] Alleine schon der Umstand, dass die „Vertrauensfrage" im Kontext des Cloud Computing permanent aufgeworfen wird, verhindert die Etablierung eines stabilen Cloud-Marktes, in dem es nicht – wie bei anderen Produkten und Dienstleistungen – um Qualität, Preis und Service, sondern um die Legitimität der Innovation als solche geht.

VII. Ausblick: Compliance- und Risikomanagement als Enabler des Cloud Computing

Betrachtet man die wesentlichen „Sales Blocker" für Cloud-Computing-Angebote, nämlich die

- Beharrungstendenzen der Rechtsordnung,
- Pauschalisierungstendenzen im politischen Diskurs,
- Abschottungstendenzen der Wirtschaftsordnung,
- Ideologisierungstendenzen der fachlichen Ebene,
- Destabilisierungstendenzen des Cloud Marketing,

dann sind es letztlich die Risiken, die Teile der Politik, Medien und Gesellschaft in der Veränderung der IT-Strukturen durch das Cloud Computing sehen bzw. prognostizieren. Diese – zumindest subjektiv wahrgenommenen – Risiken führen zu einem Abwehr- bzw. Vermeidungsverhalten der Juristen in der Anwendung und Fortentwicklung des Rechts gegenüber Innovationen. Sie bringen die Politik dazu, die notwendige Diskussion um Auswirkungen der neuen Services auf einer so hohen Abstraktionsebene zu führen, dass eine wirkliche Entscheidung vermieden wird, damit in diesem Kontext keine eigene Verantwortung übernommen werden muss. Es sind aber nicht nur technische Unsicherheiten im Hinblick auf die Verfügbarkeit, Vertraulichkeit und Integrität von Daten, die als Risiko wahrgenommen werden. Vielmehr wird der Einfluss bestimmter international agierender Player auf heimische Märkte als weiteres Risiko gesehen, was einen Schutzinstinkt gegenüber nationalen Anbietern auslöst. Schließlich kann man die Kommunikation dieser Risiken als weiteres, eigenes Risiko, nämlich jenem der Destabilisierung, begreifen.

Nachdem diese Risiken auf einer rein fachlichen und rationalen Basis nicht beseitigt werden können, und jedwede Regulierung des Cloud Computing (außerhalb eines unsinnigen und ohnehin nicht erwünschten Totalverbots) nur unvollkommene Verbindlichkeiten begründen kann, geht es aus Sicht der Cloud-Anbieter letztlich um ein adäquates Compliance- und Risikomanagement. Dieses kann Enabler des Cloud Computing sein.

1. Netzpolitisch: Schaffung neuer Vertrauensstrukturen

Die kurze Analyse der Rechtslage und der rechtspolitischen Implikationen der aktuellen Cloud-Diskussion hat gezeigt, dass Cloud Computing auf längere Sicht mit dezidierten Unsicherheitsfaktoren behaftet sein wird. Weder eine eindeutige „Öffnungsklausel" für weitergehende IT-Outsourcing-Dienste (etwa im Sinne einer Novellierung oder Ergänzung des § 11 BDSG) noch der Versuch einer strengen Regulierung zur Minimierung (etwa im Sinne einer konkretisierenden Verschärfung des § 11 Abs. 2 BDSG) sind zu erwarten. Das deshalb aus Anbietersicht vorzugswürdige Compliance- und Risikomanagement-Konzept sollte – gleichsam proaktiv – kurzfristig auf neue Vertrauensstrukturen und langfristig auf eine neue Vertrauenskultur setzen.

Vertrauen bedeutet, trotz Ungewissheit und Verwundbarkeit zu erwarten, dass andere ihre Freiräume kompetent und verantwortungsvoll nutzen.[71] Erst Vertrauen macht die Akteure in einem komplexen System wie der Cloud-Infrastruktur handlungsfähig. Notwendig ist ein generalisiertes Vertrauen, eine vertrauensvolle Grundeinstellung, die nicht Anbieter gegen Nachfrager ausspielt, sondern eine „Koalition der Verantwortungsvollen gegen Betrüger und Trittbrettfahrer" bildet.[72] Ebenso gehört eine gewisse Fehlertoleranz und eine „Kultur des konstruktiven Problemlösens" zu einer neuen Vertrauenskultur: Vertrauen wird nämlich „nicht schon dadurch zerstört, dass ein Problem auftritt, sondern erst dadurch, dass die betreffenden Akteure

[70] Dieses Phänomen könnte eventuell über eine Einbeziehung von Erkenntnissen der spieltheoretischen Vertrauensforschung erklärt werden, was an dieser Stelle nur angedeutet werden kann. Vgl. zum Einstieg *Peng-Keller*, Vertrauen verstehen, Hermeneutische Blätter 1/2–2010, S. 12 (http://www.vertrauen-verstehen.uzh.ch/personen/peng-keller/HBl2010_1_2_Peng_Keller.pdf).

[71] *Möllering*, Vernebeltes Vertrauen? Cloud Computing aus Sicht der Vertrauensforschung, 2011, S. 4, http://www.mpifg.de/people/gm/downloads/MK_Moellering_VernebeltesVertrauen_Dokumentation_100209.pdf.

[72] *Möllering*, Vernebeltes Vertrauen?, a.a.O., S. 5.

das Problem nicht lösen, sondern sich als inkompetent erweisen oder sich gar ihrer Verantwortung entziehen".[73]

Flankiert wird ein solches System durch Kontrollen, die aber den Freiraum der Akteure des vertrauenswürdigen Systems nicht in Frage stellen dürfen, sondern im Gegenteil das Vertrauen darin stärken, indem sie (alleine) den Vertrauensmissbrauch im Visier haben. Dass die Kontrolleure ihrerseits um Vertrauen werben müssen, widerspricht diesem Prinzip nicht, sondern bestätigt es.

2. Formaljuristisch: Entwicklung neuer Einwilligungsprozesse

Datenschutzrechtlich umgemünzt wird ein Compliance- und Risikomanagement beim Cloud Computing auf die Entwicklung neuer Einwilligungsprozesse setzen müssen.[74] Will man nämlich nicht alleine auf eine Rechtfertigung durch gesetzliche Ermächtigung angewiesen sein, lässt sich eine (gar hohe) Legitimation der Verlagerung von persönlichen und geschäftlichen Daten „in die Wolke" am ehesten durch Einwilligung jener erreichen[75], um deren Daten bzw. Interessen es bei dieser Datenverarbeitung geht. Weil man de lege lata aber bezweifeln kann, ob eine wirksame informierte Einwilligung durch konventionelle Datenschutzpolicies oder AGBs erzielt werden kann, gilt es, die Vorteilhaftigkeit und Vertrauenswürdigkeit der eigenen Cloud-Infrastruktur, ihrer Akteure und Prozesse, gegenüber den Betroffenen so zu verdeutlichen, dass diese ernsthaft bereit sind, die offen gelegten (Rest-)Risiken einzugehen. Die Schaffung von Transparenz ist der maßgebliche Legitimationsfaktor für eine daraufhin erteilte Einwilligung zum IT-Outsourcing.

3. Dogmatischer Rechtfertigungsansatz: Risikoabwägung i.S.d. § 9 S. 2 BDSG

Rechtsdogmatische Grundlage für das Konzept des Compliance- und Risikomanagements ist § 9 S. 2 BDSG. Danach sind Maßnahmen zur Gewährleistung von IT-Sicherheit nur erforderlich, „wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht". Das Datenschutzrecht verdeutlicht mit dieser Regelung, dass es keinen „Datenschutz um jeden Preis" gibt.[76] So ist auch bei der

[73] *Möllering*, Vernebeltes Vertrauen?, a.a.O., S. 6.

[74] Neuartige Einwilligungsprozesse werden auch bei der allgegenwärtigen Datenverarbeitung im Smart Life gefordert, vgl. dazu den Ansatz des Smart Privacy Managements, *Heckmann*, K&R 2011, 1 (5).

[75] Kritisch *Niemann/Hennrich* CR 2010, 686 (688), die davon ausgehen, dass die Einwilligung von Datensubjekten cloud-spezifisch nicht von Relevanz sein kann. Nicht nur kann diese jederzeit widerrufen werden, sondern bestehen auch Schwierigkeiten, diese durch AGB und abstrakt für alle möglichen Datenverarbeitungen in einer Cloud herbeizuführen.

[76] Dies entspricht auch der verfassungsrechtlichen Rechtsprechung, wonach der „Einzelne nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine" Daten [hat]" vgl. BVerfGE 65, 1, 43 f.

Auftragsdatenverarbeitung im Rahmen von Cloud-Computing-Diensten zur Sicherung sowohl der personenbezogenen Daten selbst als auch ihrer Verarbeitungsprozesse (nur) jenes Schutzniveau zu „gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist."[77] Dabei sind der Stand der Technik und die bei der Durchführung von Sicherungsmaßnahmen entstehenden Kosten zu berücksichtigen. Leitlinien für die Abwägung sind der konkrete Schutzbedarf und das Schadenspotenzial.[78] Dies läuft im Ergebnis auf eine Risikoanalyse heraus, weil „absolute Sicherheit in vernetzten Systemen selbst mit erheblichem Aufwand kaum erreichbar ist. Es gilt stattdessen, ausreichende Hürden gegen einen Missbrauch der Systeme und angemessene Vorkehrungen gegen Störungen zu planen, umzusetzen und regelmäßig im Hinblick auf ihre Wirksamkeit zu kontrollieren".[79]

Am Ende gilt es, ein adäquates Schutzniveau[80] für den Schutz konfligierender Interessen und Rechtsgüter zu erreichen. Dies beginnt mit einer politisch überzeugenden und rechtsdogmatisch konsistenten Bestimmung des richtigen Maßes von IT-Sicherheit bzw. Datenschutz. Das darauf aufbauende Risikomanagement-Konzept schafft Transparenz, Vertrauen und Dispositionssicherheit. Dies löst auf lange Sicht die hier vorgestellten „Sales Blocker" auf.

[77] *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2010, § 9 Rn. 19.

[78] *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2010, § 9 Rn. 21 ff.

[79] So zutreffend *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2010, § 9 Rn. 28.

[80] Hierzu grundsätzlich *Heckmann/Seidl/Maisch*, Adäquates Sicherheitsniveau in der elektronischen Kommunikation, 2012, passim.