Gerrit Hornung, Stephan Sädtler

Eitel Sonnenschein oder Wolken am Horizont?

Cloud Computing im Gesundheitswesen und die rechtlichen Schutzinstrumente der Telematik-Infrastruktur

Wie in vielen anderen Bereichen verbinden auch die Akteure im Gesundheitswesen große Hoffnungen mit dem Einsatz von Cloud Computing. Allerdings sind die rechtlichen Grenzen und Unklarheiten hier sogar noch größer als in anderen Bereichen der vernetzten Datenverarbeitung. Vor diesem Hintergrund geht der Beitrag den rechtlichen Anforderungen an den Einsatz von „Gesundheits-Clouds" und insbesondere der Frage nach, ob Regelungsansätze der Gesundheits-Telematik übertragbar sind.

1 Einleitung

Cloud Computing ist derzeit eine der am stärksten diskutierten technischen Innovationen. Die Technologie bietet vielfältigste Einsatzmöglichkeiten und zielt im Kern darauf ab, einen fein-skalierbaren Zugriff auf zentral verwaltete IT-Ressourcen in Form von Speicherplatz, Software, Rechenleistung oder ganzen Infrastrukturen zu ermöglichen.[1] Nahezu sämtliche private IT-Branchen und viele Stellen des öffentlichen Sektors machen sich Gedanken darüber, wie sie Cloud Anwendungen am besten für sich nutzen können[2] und versuchen, eigene Cloud-Strategien zu entwickeln bzw. kontinuierlich zu optimieren.

Die Bedeutung wird dadurch unterstrichen, dass das Bundesministerium für Wirtschaft und Technologie (BMWi) mit dem Technologieprogramm „Trusted Cloud" derzeit insgesamt 14 Forschungsprojekte mit dem Ziel eines „innovativen, sicheren und rechtskonformen Cloud Computing"[3] fördert. Von diesen stammen drei Projekte direkt aus dem Gesundheitssektor, und auch ansonsten existieren vielseitige Ideen und Ansätze, wie die Qualität der Gesundheitsversorgung mittels Cloud Anwendungen verbessert werden könnte.[4]

Daneben gibt es Infrastrukturmodelle und Anwendungen, die nicht unmittelbar aus dem „Cloud-Gedanken" heraus geboren wurden, in Zukunft aber Cloud Elemente enthalten könnten. Ein Beispiel hierfür ist die Telematik-Infrastruktur, deren Ziel der „Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung" gemäß § 291a Abs. 1 SGB V[5] mittels „vereinfachter Verwaltungsabläufe" und hoher „Verfügbarkeit medizinischer Informationen"[6] stark an die Ziele des Cloud Computings erinnert. Interessanterweise hat der Gesetzgeber bei der Verabschiedung der rechtlichen Grundlagen zwei Probleme adressiert, die auch in der Diskussion um das Cloud Computing in sensiblen Einsatzbereichen immer wieder identifiziert werden, nämlich die sichere Authentisierung und den Beschlagnahmeschutz. Vor diesem Hintergrund soll im Folgenden ein erster Blick auf den Ein-

1 S. dazu *BSI*, https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen /Grundlagen_node.html; *BITKOM*, Cloud Computing – Evolution in der Technik, Revolution im Business, 2009.; *AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe Cloud Computing, 2011. Der Text ist im Zusammenhang mit dem BMWi-geförderten Projekt „SkIDentity – Vertrauenswürdige Identitäten für die Cloud" FKZ 01/1011031, entstanden.

Prof. Dr. Gerrit Hornung, LL.M.

Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Direktor am dortigen Institute of IT-Security and Security Law (ISL).
E-Mail: Gerrit.Hornung@uni-passau.de

Stephan Sädtler

Wissenschaftlicher Mitarbeiter am genannten Lehrstuhl und Fachanwalt für IT-Recht.

E-Mail: Stephan.Saedtler@uni-passau.de

2 Laut einer BITKOM Umfrage vom 7.3.2012 nutzt jedes vierte Unternehmen in Deutschland Cloud Computing, http://www.bitkom.org/de/presse/8477_71446.aspx; s.a. *Schröder/Haag*, ZD 2012, 495.

3 S. http://www.trusted-cloud.de/.

4 So waren Cloud Lösungen Thema der weltgrößte Medizinmesse MEDICA 2012.

5 Die Ziele (s. z.B. *Hornung*, Die digitale Identität, 2005, 41 ff. m.w.N.) beziehen sich dort auf die Gesundheitskarte, die aber nur ein Baustein der Infrastruktur ist.

6 http://www.gematik.de/cms/de/egk_2/ziele/ziele_1.jsp.

satz von Cloud Computing in der Gesundheits-Telematik und in anderen Gesundheitsanwendungen geworfen und der Frage nachgegangen werden, ob die Lösungen des Gesetzgebers verallgemeinerungsfähig sind.

2 Cloud Computing

Eine einheitliche „Cloud-Definition" existiert bisher nicht. Zur Veranschaulichung kann die häufig verwendete Definition der US-amerikanischen Standardisierungsstelle NIST (National Institute of Standards and Technology) dienen: „Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."[7] Charakteristisch ist die auf den Bedarf zugeschnittene Zugriffsmöglichkeit einer unbestimmten Anzahl von Nutzern auf die Ressourcenangebote zentraler Anbieter, die in Komplettlösungen oder individuellen, anpassungsfähigen Diensten bestehen können.[8]

Dabei haben sich bisher die drei Obergruppen „Infrastruktur as a Service" (IaaS), „Plattform as a Service" (PaaS) und „Software as a Service" (SaaS) herausgebildet,[9] welche u.a. die verschiedenen Abstufungen in der technischen Verantwortlichkeit des Kunden im Rahmen der einzelnen Cloud Anwendungen beschreiben. Am unteren Ende des Spektrums befinden sich IaaS Anwendungen, bei denen ein Kunde lediglich in standardisierter Form Speicherplatz und Rechenleistung von einem Anbieter beziehen kann, der es ihm ermöglicht, eigene Anwendungen in die Cloud zu verlagern. Am anderen Ende wird dem Kunden in Form von SaaS eine Komplett-Anwendung als Endprodukt aus der „Wolke" angeboten. Dazwischen sind PaaS Anwendungen angesiedelt, bei denen Nutzer Plattformen vorfinden, die sie noch nach ihren individuellen Bedürfnissen mit eigenen Anwendungen kombinieren bzw. anpassen können. Die Vielfalt von Cloud Angeboten wird häufig durch die Bezeichnung „X" as a Service (XaaS), zum Ausdruck gebracht.

Zu unterscheiden sind private und öffentliche Clouds. Während „Public Clouds" grundsätzlich von jedermann bzw. von einem unbestimmten Personenkreis genutzt werden können, ist eine „Private Cloud" nur einer bestimmten Personengruppe wie den Mitarbeitern eines einzigen Unternehmens, Konzerns oder Behörde zugänglich. Technisch müssen sich die beiden Formen nicht zwangsläufig unterscheiden; es existieren auch Mischformen. Eine weitere Differenzierung kann zwischen der Nutzung von Cloud Anwendungen durch Private einerseits, die öffentliche Verwaltung andererseits erfolgen, da Letzterem deutlich engere rechtliche Grenzen gesetzt sind.[10]

Die Vorteile des Cloud Computings für Cloud Nutzer bestehen in dem scheinbar grenzenlosen, ortsunabhängigen, bedarfsgerechten und kostengünstigen Zugriff auf Software, Speicherplatz und Rechenleistung sowie den damit verbundenen „Support-Dienstleistungen". Davon profitieren sowohl Nutzer, die standardisierte Massenanwendungen auslagern, als auch solche, die bestimmte Ressourcen wie Speicherplatz, Softwarelizenzen oder Rechenleistung nur selten benötigen und so in die Lage versetzt werden, Prozesse kostengünstiger oder sogar erstmals durchführen zu können. Die Vorteile für Cloud Anbieter bestehen hingegen vornehmlich in einer erheblichen Optimierung der eigenen Kapazitäten.[11]

Cloud Computing kann einerseits die IT-Sicherheit erhöhen, da gerade KMUs aufgrund des Kostenvorteils ein höheres Sicherheitsniveau anbieten können.[12] Umgekehrt kann jedoch ein wesentliches Risiko des Cloud Computings auf technischer Ebene in dem Verlust an Kontrolle und Transparenz liegen, da Nutzer sich eines externen Dienstleisters und dessen Infrastruktur bedienen und dieser wiederum typischerweise Subunternehmer be-

7 Übersetzung des *BSI* (Fn. 1).

8 S. hierzu z.B. *Metzger/Reitz/Villar*, Cloud Computing. Chancen und Risiken aus technischer und unternehmerischer Sicht, 2011.

9 S. zu den Grundlagen z.B. *BITKOM* (Fn. 1), 22 ff.; *BSI*, Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter, 2010, 14 ff.

10 Dazu *Schulz*, MMR 2010, 75.

11 S. *BITKOM* (Fn. 1), 44 ff.

12 S. *Article 29 Data Protection Working Party*, Opinion 05/2012 on Cloud Computing, 2012, 4; *Schröder/Haag*, ZD 2012, 495, 496.

auftragt. So können die Kapazitäten von Cloud Providern über den ganzen Globus verteilt sein. Zudem bringen die Zugriffsmöglichkeiten einer oft unbeschränkten Anzahl von Personen – sog. Mandantenfähigkeit – ein erhebliches Sicherheitsrisiko mit sich.[13]

3 Der Einsatz von Cloud Computing im Gesundheitssektor

3.1 Ausgangspunkt

Der vielseitige Nutzen gerade im Gesundheitssektor lässt sich an verschiedenen Forschungsprojekten verdeutlichen. Die Hoffnungen sind groß: „Konsolidierte Patientendaten können zur Identifikation von Krankheitsmechanismen beitragen, Rekrutierungszeiten von Patienten in klinischen Studien reduzieren, die Überwachung von Medikamentensicherheit durch kontinuierliches Monitoring verbessern, Plausibilitätsprüfungen des ärztlichen Handelns effizient und kostengünstig ermöglichen und einen Beitrag zur Entbürokratisierung im Abrechnungswesen des deutschen Gesundheitssystems leisten".[14]

In diesem Sinne hat sich das Projekt „Coud4health" die Sammlung und Auswertung von großen Rohdatenbeständen zur Optimierung der medizinischen Forschung zum Ziel gesetzt,[15] „Genecloud" soll „mittelständischen Unternehmen über die Cloud Zugang zu Methoden erlauben, die eine schnellere und effizientere Entwicklung von medizinischen Wirkstoffen ermöglichen",[16] „TRESOR" zielt auf die Realisierung eines modernen, schnellen, umfänglichen und v.a. sicheren Datenaustauschs von Diagnostik und Behandlungsdaten beispielsweise zwischen den einzelnen Stellen einer Behandlungskette.[17] Weitere Forschungsprojekte befassen sich z.B. mit der Datenverarbeitung in der mobilen Pflege,[18] der Langzeitarchivierung medizinischer Datensätze mittels einer Storage aaS Anwendung[19] oder der Online-Beratung bestimmter Patientengruppen, bei der Daten und Software zentral auf dem Server des Anbieters gespeichert sind, was einen ortsunabhängigen Zugriff und eine nutzungsabhängige Berechnung (in Bezug auf die Software) ermöglicht.[20] Allen Projekten ist gemeinsam, dass sie durch die zentrale Datensammlung, Verarbeitung und Auswertung sowie die damit verbundenen Zugriffsmöglichkeiten die Verbesserung von Behandlung und Forschung zum Ziel haben. Die Vorteile scheinen dabei auf der Hand zu liegen, die vorgebrachten Argumente plausibel.

3.2 Der Vergleich mit der Telematik-Infrastruktur

Die Telematik-Infrastruktur mit ihrem Herzstück, der elektronischen Gesundheitskarte,[21] wurde zu einem Zeitpunkt geplant, zu dem „Cloud Computing" höchstens Eingeweihten ein Begriff war. Betrachtet man die Pläne allerdings vor dem Hintergrund der oben genannten Definitionen, so ergeben sich einige Parallelen. Die „interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur", die nach § 291a Abs. 7 Satz 1 SGB V geschaffen werden soll, dient der Erbringung der Pflicht- und Wahlanwendungen der Gesundheitskarte nach § 291a Abs. 2 und Abs. 3 SGB V.[22] Zumindest die datenintensiven Anwendungen, insbesondere die elektronische Patientenakte, werden auf serverbasierte Lösungen angewiesen sein und erfordern die effiziente, dauerhafte und verteilte Speicherung von Daten, die für eine Vielzahl von zugriffsberechtigten Leistungserbringern verfügbar gehalten werden müssen.

Je mehr Daten in dieser Weise erhoben, verarbeitet und genutzt werden, desto mehr wird es aus der Infrastrukturperspektive darauf ankommen, die verfügbaren Ressourcen möglichst effizient auszunutzen und den nutzungsberechtigten Leistungserbringern bedarfsorientiert zur Verfügung zu stellen. Zum jetzigen Zeitpunkt ist zwar immer noch nicht endgültig entschieden, welche Basistechnologien und Komponenten in der Telematik-Infrastruktur eingesetzt werden sollen.[23] Angesichts der beschriebenen Aufgabenstellung erscheint es aber nicht unwahrscheinlich, dass mittelfristig zumindest bei daten- und rechenintensiven Diensten gängige Cloud-Technologien zum Einsatz kommen. Werden Daten zentral oder in verteilten, aber allen Berechtigten über Web-Applikation offenstehenden Systemen gespeichert und verarbeitet, betrifft dies Storage aaS, das Bestandteil aller Cloud Typen (SaaS, PaaS, IaaS) sein kann. Wird darüber hinaus der einzelnen Stelle eine Anwender-Software zur Datenverarbeitung bereitgestellt, wäre dies als Software aaS zu klassifizieren.

Natürlich sollten die verbleibenden Unterschiede nicht übersehen werden: Schon wegen der Dokumentationspflichten und der mit ihnen verbundenen Haftungsrisiken wird jeder Leistungserbringer bis auf weiteres lokale, authentische Kopien seiner Daten vorhalten müssen.[24] Es ist auch keine das gesamte deutsche Gesundheitswesen umfassende zentrale Cloud-Lösung geplant, in der sensible Patientendaten verschwinden. Ebenso wird es nicht möglich sein, das volle Cloud Potential auszuschöpfen, das normalerweise durch die optimierte Ressourcen-Auslastung aufgrund der flexiblen Allokationsmöglichkeiten von Daten und Software entsteht. All das schließt den Einsatz von Cloud Anwendungen aber jedenfalls technisch nicht aus. Es erscheint also möglich, dass die Telematik-Infrastruktur nach und nach Elemente einer umfassenden „Gesundheits-Cloud" enthalten wird, die zumindest potentiell alle Leistungserbringer und – vorbehalt-

13 S. zu den Nachteilen und Risiken *Article 29 Data Protection Working Party* (Fn. 12), 2.

14 So Prof. Marquard, Universitätsklinikum Gießen und Marburg, http://www.medica.de/cgi-bin/md_medica/custom/pub/content.cgi?lang=1&oid=24744&ticket=09954318481058&ca_page=de%2Fpr_info_specarticles_fa03d.html.

15 S. http://www.trusted-cloud.de/de/772.php.

16 S. http://www.trusted-cloud.de/de/791.php.

17 S. http://www.trusted-cloud.de/de/764.php.

18 S. *Herkenhöner/Fischer/de Meer,* DuD 2011, 870.

19 S. http://www.medizin-edv.de/archivierung/modules/AMS/article.php?storyid=97.

20 S. die Plattform „Synx", die übergewichtigen Jugendlichen ein entsprechendes Online-Coaching bieten soll (http://www.microsoft.com/germany/newsroom/pressemitteilung.mspx?id=533335).

21 Dazu z.B. *Weichert*, DuD 2004, 391 ff.; *Hornung* (Fn. 5), 58 ff., 207 ff., 246 ff., 362 ff.; *ders*., in: Hänlein/Kruse/Schuler, LPK-SGB V, 4. A. 2012, § 291a, Rn. 1 ff.; *Borchers*, Die Einführung der elektronischen Gesundheitskarte in das deutsche Gesundheitswesen, 2008; *Duttge/Dochow* (Hrsg.), Gute Karten für die Zukunft? Die Einführung der elektronischen Gesundheitskarte, 2009.

22 Dazu aus rechtlicher Sicht z.B. *Hornung* (Fn. 5), 60 ff.; *Bales/Dierks/Holland/Müller,* Die elektronische Gesundheitskarte, 2007, 80 ff.; *Dierks/Püschel*, in: Duttge/Dochow (Fn. 21), 27 ff.

23 Zu Hintergründen und „Status Quo" *TeleTrusT,* Thesenpapier zur Gesundheitstelematik, 2012.

24 S. *Hornung* (Fn. 5), 213 ff. m.w.N.; zu den haftungsrechtlichen Auswirkungen der Dokumentationspflicht *Wellner*, in: Geigl, Haftpflichtprozess, 26. A. 2011, Rn. 266 ff.; *Steinhilper* in Laufs/Kern, Handbuch des Arztrechts, 4. A. 2010, 125 Rn. 28 ff.

lich der Einwilligung[25] – alle Inhaber der Gesundheitskarte umfassen wird.

Mit dieser Einordnung sind zunächst keinerlei Rechtsfolgen verbunden. Vielmehr verdeutlichen gerade die vorstehenden Überlegungen, dass es kaum möglich ist, generelle Anforderungen an „das" Cloud Computing zu formulieren, weil die eingesetzten Technologien und Konfigurationen, die Beteiligten und ihre Interessen, die Geschäftsmodelle und gesetzlichen Aufgaben der Datenverarbeiter und schließlich bestimmte spezialgesetzliche Anforderungen ein zu heteronomes Bild ergeben. Die Telematik-Infrastruktur sperrt sich auch gegen gängige Kategorisierungen: Einerseits könnte man beim Cloud-Einsatz wegen der Zugriffsbeschränkungen auf den Kreis der Berechtigten in § 291a Abs. 4 Satz 1 SGB V[26] von einer „privaten" Cloud sprechen – angesichts von über 300.000 Ärzten in Deutschland nebst Hilfspersonal aber im Ergebnis nur deswegen, weil zum Datenzugriff die Mitwirkung des Patienten erforderlich ist. Auch hinsichtlich der Unterscheidung zwischen hoheitlichen und privaten Clouds läge eine Mischlösung vor: Die Datenstrukturen werden gesetzlich reguliert und betreffen zunächst nur die gesetzlich Versicherten.[27] Im Bereich der Leistungserbringer werden aber vielfach private Stellen die Infrastruktur nutzen.

4 Anforderungen an das Cloud Computing

Der rasante technologische Fortschritt stellt Cloud Anbieter und Nutzer sowie Rechtsanwender vor erhebliche Herausforderungen. Aufgrund der Beauftragung externer Dienstleister und deren weltweit verteilter Subunternehmer stellen sich Probleme der Auftragsdatenverarbeitung und des grenzüberschreitenden Datenverkehrs in Staaten außerhalb der EU bzw. des EWR. Durch die hohe Flexibilität von Cloud-Systemen treten daneben Schwierigkeiten bei der Dokumentation, den Kontrollpflichten und -rechten sowie den Transparenzanforderungen auf.[28]

Auf die Verarbeitung durch einen Cloud Provider finden nach h.M. die Regeln über die Auftragsdatenverarbeitung (§ 11 BDSG) Anwendung.[29] Der Provider ist damit kein „Dritter" (§ 3 Abs. 8 Satz 3 BDSG) und der Datentransfer an ihn keine Übermittlung (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG), sodass es hierfür keiner gesonderten Erlaubnis bedarf, soweit die Daten innerhalb der EU bzw. des EWR verbleiben. Ungelöst ist derzeit allerdings, wie ein Auftraggeber seinen nach § 11 i.V.m. § 9 BDSG auferlegten Kontrollpflichten in den abgeschotteten und weltweit verteilten Rechenzentren nachkommen soll, und wie ein Cloud Anbieter dem Transparenzgebot ausreichend Rechnung tragen kann.[30] Soweit Sozialdaten (§ 67 Abs. 1 SGB X) betroffen sind, gelten starke Einschränkungen für die Verarbeitung durch private Stellen – u.a. die Voraussetzung, dass der überwiegenden Teil des Datenbestandes beim Auftraggeber verbleiben muss (§ 80 Abs. 5 Nr. 2 SGB X). Dies wird in gängigen Cloud Anwendungen nicht gewährleistet, sodass deren Nutzung insoweit unabhängig von einer Übermittlung ins Ausland derzeit nicht in Betracht kommt.

Findet zudem noch ein für das Cloud Computing nicht untypischer Transfer in Drittstaaten außerhalb der EU bzw. des EWR statt, gilt die Privilegierung des § 3 Abs. 8 Satz 3 BDSG nicht. Schon die Rechtmäßigkeit für diesen Transfer ist aufgrund der zweifelhaften Erforderlichkeit einer solchen Maßnahme i.S.v. § 28 Abs. 1 BDSG umstritten;[31] zudem müssen zusätzlich die Anforderungen der §§ 4b, 4c BDSG erfüllt sein. Ein angemessenes Schutzniveau im Empfängerstaat kann dies erfüllen, scheidet aber aufgrund drittstaatlicher Zugriffsbefugnisse und fehlender Schutzstandards, Betroffenenrechte und Aufsichtsbefugnisse in vielen Fällen aus.[32] Eine Übermittlung in Drittsaaten kann deshalb nur über die Vereinbarung von Standardvertragsklauseln bzw. konzernintern durch verbindliche Unternehmensregelungen rechtskonform gestaltet werden kann. Möglich sind auch Einwilligungslösungen, sofern die Anforderungen der Informiertheit und Freiwilligkeit eingehalten werden und sich die Einwilligung nach § 4a Abs. 3 BSDG explizit auf die Gesundheitsdaten als besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) bezieht.

Aufgrund von § 3 Abs. 9 BDSG gelten überdies die weiteren Einschränkungen nach § 28 Abs. 6 bis 9 BDSG. Für die Verarbeitung und Nutzung von Gesundheitsdaten ordnet § 28 Abs. 7 Satz 2 BDSG die Subsidiarität gegenüber der ärztlichen Schweigepflicht an, die beim Einsatz von Cloud Computing wie bei jedem Umgang mit Gesundheitsdaten zu beachten ist. Sie ergibt sich aus drei Rechtsgrundlagen, nämlich § 203 Abs. 1 Nr. 1 StGB, der standesrechtlichen Norm des § 9 MBO-Ä und dem Behandlungsvertrag. Die Schweigepflicht ist Grundlage für eine vom Vertrauen des Patienten getragene wirkungsvolle ärztliche Behandlung und insofern „Grundvoraussetzung ärztlichen Wirkens", weil sie „die Chancen der Heilung vergrößert und insgesamt der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient".[33] Unzulässig und nach § 203 StGB strafbar ist das unbefugte Offenbaren von Patientendaten, zu denen bereits die Tatsache eines Arztbesuchs und der Name des Patienten zählen.[34] Setzt der Schweigepflichtige demgegenüber lediglich Gehilfen ein, die er kontrollieren kann, liegt keine Offenbarung vor;[35] hier besteht wegen der eigenen Strafbarkeit der Gehilfen nach § 203 Abs. 3 Satz 2 StGB ausreichend Schutz.[36]

25 Diese ist bei den hier relevanten Anwendungen nach § 291a Abs. 3 und Abs. 5 SGB V erforderlich; dazu *Hornung* (Fn. 5), 212 ff.

26 Einzelheiten bei *Hornung* (Fn. 5), 220 ff.

27 Die Teilnahme der PKV ist optional, s. § 291a Abs. 1a SGB V.

28 S. zum Ganzen z.B. *Article 29 Data Protection Working Party* (Fn. 12); *AK Technik und Medien* (Fn. 1), *Hornung/Sädtler,* CR 2012, 683; *Schmidt-Bens,* Cloud Computing Technologien und Datenschutz, 2012; *Stogmöller*, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2. A. 2011, Teil 5, Rn. 350 ff.; *Heidrich/Wegener*, MMR 2010, 803; *Weichert*, DuD 2010, 679.

29 S. u.a. *Gola/Schomerus*, BDSG, 11. A. 2012, § 11 Rn. 8; *Petri*, in: Simitis, BDSG, 7. A. 2011, § 11 Rn. 30; *Weichert*, DuD 2010, 679, 682.

30 S.a. *Weichert*, DuD 2010, 679, 682 f.; s. hierzu die Reformvorschläge der *AG Rechtsrahmen des Technologieprogrammes „Trusted Cloud"*, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, 6 ff.

31 S. *Schmidt-Bens* (Fn. 28), 70 ff.

32 S. im Zusammenhang mit den USA und Safe Harbor *Düsseldorfer Kreis,* Beschluss vom 28./29.04 2010, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html?nn=409242; zum Ganzen *Schneider*, in: Taeger (Hrsg.), IT und Internet – mit Recht gestalten, 2012, 759; *Hansen*, DuD 2012, 407, 410 f.

33 BVerfGE 32, 373 (380).

34 LG Köln, NJW 1959, 1598, 1599; OLG Oldenburg, NJW 1982, 2615, 2616; *Vahle*, DuD 1991, 614, 615; *Taupitz*, MDR 1992, 421, 424.

35 *Kilian*, NJW 1987, 695, 697; *Inhester,* NJW 1995, 685, 688; *Geis*, DuD 1997, 582, 586 f.; die Auswirkungen einer Auftragsdatenverarbeitung auf § 203 StGB sind ungeklärt (*Dierks*, in: *TeleTrusT* (Fn. 23), 67); gegen eine Vergleichbarkeit *Kroschwald/Wicker,* in: Taeger (Fn. 32) 733, 747; a.A. *Hehgmanns/Niehaus*, NStZ 2008, 57, 62.

36 S. *Bräutigam*, CR 2011, 411, 413 mit Verweis u.a. auf *Lenckner/Eisele*, in: Schönke/Schröder, StGB, 28. A. 2010, § 203 Rn. 64 und *Lensdorf/Mayer-Wegeling/Mantz*, CR 2009, 62, 64.

Für die Telematik-Infrastruktur[37] wie für den Einsatz von Cloud-Technologien in anderen Gesundheitsbereichen bedeutet dies, dass regelmäßig von einem Offenbaren auszugehen ist.[38] Eine Gehilfenstellung im strafrechtlichen Sinn ist bei professionellen Cloud Anbietern nicht zu bejahen. Sie ist schon beim Einsatz externen IT-Wartungspersonals umstritten.[39] Soweit ein Teil der Literatur Outsourcing-Dienstleister als Gehilfen anerkennt, werden jedenfalls Steuerungs-, Weisungs- und Kontrollrecht des Geheimnisträgers verlangt.[40] Diese sind bei typischen Cloud Anwendungen nicht gegeben.

Eine Strafbarkeit kann damit nur auf zwei Wegen vermieden werden. Entweder wird das Offenbaren technisch durch hochsichere Verschlüsselungsverfahren ausgeschlossen.[41] Oder es muss eine entsprechende Befugnis des Schweigepflichtigen geschaffen werden, die in einer Einwilligung der Patienten oder in gesetzlichen Regelungen liegen kann. Einwilligungslösungen erscheinen für spezifische Cloud Anwendungen (z.B. bei daten- und rechenintensiven Spezialbehandlungen) möglich; angesichts der datenschutzrechtlichen Risiken und der Möglichkeit des Einholens einer ausdrücklichen Einwilligung kann sie aber nicht als mutmaßliche oder konkludente Erklärung konstruiert werden.[42] Für größere Patientengruppen wäre eine gesetzliche Regelung erforderlich, die zum Schutz der Grundrechte der Patienten auf Gesundheit und informationelle Selbstbestimmung effektive IT-Sicherheitsmaßnahmen vorsehen müsste.

Im Ergebnis werden Cloud Lösungen im Gesundheitswesen damit – von Einzelfällen der Einwilligung abgesehen – nur mit Daten möglich sein, die bereits durch die Schweigepflichtigen verschlüsselt werden und so nicht nur auf den Transportwegen, sondern auch gegen den Zugriff des Cloud Anbieters geschützt sind. Zusätzlich stellt sich das Problem der teilweise langfristigen Aufbewahrungspflichten von Gesundheitsdaten (bis zu 30 Jahre,[43] in Extremfällen sogar noch länger[44]). Es lässt sich technisch kaum garantieren, dass heutige Verschlüsselungsverfahren so lange sicher sind. Deshalb könnte trotz heute sicherer Verfahren bereits zum Zeitpunkt der (verschlüsselten) Übermittlung ein Offenbaren vorliegen und damit ein Strafbarkeitsrisiko entstehen.

Neben der Verschlüsselung sind daher Lösungen mittels Pseudonymisierung bzw. Anonymisierung der Gesundheitsdaten denkbar. Ein Ansatz hierzu liefert das Modell einer „elektronischen Datentreuhänderschaft", das die Pseudonymisierung von Patientenlisten durch einen rechtlich selbständigen, unabhängigen und vertrauenswürdigen Dritten vorsieht.[45] Bei der verarbeitenden Stelle lägen die Behandlungsdaten damit in (datenschutzrechtlich) anonymisierter Form gemäß § 3 Abs. 6 BDSG vor, da nach h.M.[46] für eine Anonymisierung ausschlaggebend ist, dass lediglich die jeweilige verantwortliche Stelle den Personenbezug nicht herstellen kann. Soweit durch entsprechende Maßnahmen eine Re-Individualisierung ausgeschlossen ist, unterfallen die Behandlungsdaten nicht mehr dem Datenschutzrecht; bei ausreichender Anonymisierung scheidet auch eine Strafbarkeit nach § 203 StGB aus.[47]

5 Besondere Anforderungen und ihre Lösung im Bereich der Telematik-Infrastruktur

Wenn in vernetzten Infrastrukturen sensible personenbezogene Daten verarbeitet werden, müssen besonders hohe technische und rechtliche Schutzmaßnahmen ergriffen werden. Da Gesundheitsdaten zu den sensibelsten personenbezogenen Daten überhaupt gehören und die Verarbeitung in Cloud Computing Anwendungen durch spezifische Risiken und strukturelle Unübersichtlichkeit für die professionellen Nutzer (v.a. die Leistungserbringer) und die Betroffenen geprägt ist, gilt dies in Gesundheits-Clouds in besonderem Maße.

Unabhängig davon, ob in der Telematik-Infrastruktur bereits kurzfristig Cloud-Technologien eingesetzt werden, ergeben sich dort ähnliche Probleme. Während der Gesetzgeber auf detaillierte Vorgaben für die Verschlüsselung verzichtet hat (vorgegeben ist nach § 291 Abs. 2a Satz 4 SGB V lediglich die technische Eignung der Gesundheitskarte hierfür), finden sich detaillierte Regelungen für zwei andere Probleme: die technische Absicherung des Zugriffs durch sichere Authentisierungsverfahren und rechtliche Regelungen zum Beschlagnahmeschutz.

Sowohl aus Gründen des Patientengeheimnisses als auch des Datenschutzes insgesamt ist es erforderlich, den Zugriff auf Gesundheitsdaten in Cloud Lösungen auf die unmittelbar Zugriffsberechtigten zu beschränken. Dies kann man schon aus allgemeinen Vorgaben zur Datensicherheit (§ 9 BDSG und Nr. 3 und 4 der Anlage) ableiten, ist hier aber explizit durch § 291a Abs. 5 Satz 3 SGB V vorgeschrieben, der (neben dem Erfordernis der technischen Autorisierung durch den Versicherten in § 291a Abs. 5 Satz 2 SGB V) den Zugriff technisch auf Inhaber eines elektronischen Heilberufsausweises oder entsprechenden Berufsausweises beschränkt.[48] Dieses Erfordernis einer „starken" (d.h. chipkartenbasierten) Authentisierung wird allgemein im Bereich des Cloud Computings explizit durch das Bundesamt für Sicherheit in der Informationstechnologie (BSI) empfohlen.[49]

Gesundheits-Clouds werden also auch jenseits der expliziten Formulierung in § 291a Abs. 5 SGB V entsprechende starke Authentisierungsverfahren erfordern. Dazu müssen nicht zwingend

37 S. zur Analyse von § 203 StGB mit Blick auf die Infrastruktur und die Gesundheitskarte *Hornung* (Fn. 5), 229 ff.; *Borchers* (Fn. 21), 133 ff.

38 Auf die tatsächliche Kenntnisnahme kommt es nicht an, s. *Kroschwald/Wicker* (Fn. 35), 742 f.; *Lenckner/Eisele* (Fn. 36), § 203 Rn. 19.

39 Für die Zulässigkeit *Ulsenheimer/Heinemann*, MedR 1999, 197, 202 (mutmaßliche Einwilligung); im Ergebnis auch *Kargl*, in Kindhäuser/Neumann/Paeffgen, StGB, 3. A. 2010, § 203 Rn. 21; soweit Dritte bei der Wartung keine Kenntnis von den Geheimnissen erlangen können auch *Lensdorf/Mayer-Wegelin/Mantz*, CR 2009, 62, 63; grds. a.A. *Bäumler*, MedR 1998, 400; *Wienke/Sauerborn*, MedR 2000, 517, 518 f. (keine effektive Überwachung durch den Arzt möglich); *Kühl*, in: Lackner/Kühl, StGB, 27. A. 2011, § 203 Rn. 11b (mit Ausnahme bei Einbindung in die Praxisorganisation); *Lencker/Eisele* (Fn. 36), § 203 Rn. 64a.

40 S. *Honiek/Hülsdunk*, MMR 2004, 788; *Heghmanns/Niehaus*, NStZ 2008, 57, 59 f.; *Lendsdorf/Mayer-Wegelin/Mantz* 2009, 62, 64; *Maisch/Seidl*, DSB 2012, 127; eine Offenbarung liegt z.B. bei Outsourcing-Modellen im Abrechnungsbereich vor, s. BGH, NJW 1991, 2955.

41 S. für die Telematik-Infrastruktur *Hornung* (Fn. 5), 231; für das Cloud Computing *Kroschwald/Wicker* (Fn. 35) 741 u. 743; für das Outsourcing *Jandt/Roßnagel/Wilke*, NZS 2011, 641, 645; im öffentlich-rechtlichen Bereich wird eine Verschlüsselung explizit z.B. zum Schutze des Steuergeheimnisses in § 87a Abs. 1 Satz 1 AO für die elektronische Kommunikation der Finanzbehörden vorgeschrieben.

42 S. *Kroschwald/Wicker* (Fn. 35), 748 f. m.w.N.

43 S. eine Übersicht hierzu unter http://www.kvhb.de/aufbewahrungsfristen.

44 S. § 42 Abs. 1 StrlSchV: Aufbewahrung bis zur Vollendung des 75. Lebensjahres.

45 S. für das Beispiel eines Einsatzes im Forschungsumfeld *Dierks*, Rechtsgutachten zur elektronischen Datentreuhänderschaft im Auftrag der TMF, 2008.

46 S. *Gola/Schomerus*, (Fn. 29), § 3, Rn. 10; a.A. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. A. 2010, §3 Rn. 13.

47 S. *Lensdorf/Mayer-Weglin/Mantz*, CR 2009, 62, 67 f.

48 Zu den Einzelheiten und verbleibenden Restrisiken s. *Hornung* (Fn. 5), 221 ff.

49 S. *BSI* (Fn. 9), 43 ff.; s.a. *Hornung*, in: v. Lucke (Hrsg.), Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur 2011, 103 f.

Gesundheitskarten und elektronische Heilberufsausweise eingesetzt werden. Zumindest innerhalb des Gesundheitswesens wird sich dies allerdings regelmäßig anbieten und entspricht auch der Zweckbestimmung der Gesundheitskarte. Da ihre Einsatzzwecke allerdings in § 291 Abs. 1 Satz 2 i.V.m. § 291a SGB V abschließend geregelt sind, müssen Cloud Lösungen unter die dort erwähnten Anwendungen subsumierbar sein. V.a. im Hinblick auf die elektronische Patientenakte dürfte dies für allgemeine Gesundheits-Clouds regelmäßig zutreffen. Dagegen ist die Verwendung von Behandlungsdaten zu Forschungszwecken de lege lata durch § 291a Abs. 8 Satz 1 SGB V ausgeschlossen.[50] In diesem sowie in allen anderen Fällen, in denen die Cloud Anwendungen über die Zwecke der Behandlung hinausreichen, sind andere (starke) Authentisierungslösungen zu verwenden, die beispielsweise der neue Personalausweis bereitstellt.[51]

Technische Schutzmechanismen sind im Gesundheitsbereich unabdingbar, alleine aber nicht hinreichend. In bestimmten Bereichen müssen sie vielmehr durch rechtliche Instrumente ergänzt werden. Da dem – oftmals größeren – Kreis von Berechtigten der Zugriff eröffnet bleiben muss und im Interesse einer effektiven Gesundheitsversorgung das Vertrauen des Patienten in die Geheimhaltung seiner Daten unabdingbar ist, bedarf es der Schweigepflicht und eines effektiven Beschlagnahmeschutzes ärztlicher Aufzeichnungen als flankierende rechtliche Maßnahmen. Herkömmlich wird der Beschlagnahmeschutz an den Gewahrsam eines Zeugnisverweigerungsberechtigten geknüpft. Der Gewahrsam liegt allerdings weder in der Telematik-Infrastruktur noch im Cloud Computing vor, soweit nicht die gesamte technische Infrastruktur, v.a. aber die Datenspeicher durch Berufsgeheimnisträger betrieben werden.

Zur Lösung dieses Problems hat der Gesetzgeber den Beschlagnahmeschutz bei der Gesundheits-Telematik in zweifacher Weise „verlängert".[52] Zum einen ist die Karte selbst gemäß § 97 Abs. 2 Satz 1 StPO gewahrsamsunabhängig beschlagnahmefrei. Zum anderen erstreckt sich der Beschlagnahmeschutz nach § 97 Abs. 2 Satz 2 StPO – sehr weit formuliert – auch auf Gegenstände bei Dienstleistern, die für Heilberufsausübende Daten erheben, verarbeiten oder nutzen. Dies umfasst sämtliche Dienstleister im Zusammenhang mit der Gesundheitskarte,[53] nach umstrittener Ansicht auch deren Unterauftragnehmer.[54]

Erfasst sind auch alle Provider von Gesundheits-Clouds, wenn sie die Daten (als „Gegenstände" i.S.v. § 97 Abs. 2 Satz 2 StPO[55]) als Dienstleister im Auftrag erheben, verarbeiten und nutzen.[56] Die Regelung wurde zwar zusammen mit der Einführung der Gesundheitskarte geschaffen, weder aus Wortlaut noch Gesetzesbegründung ergibt sich jedoch, dass sie lediglich Dienstleister im Zusammenhang mit der Gesundheits-Telematik erfassen soll.[57] Eine Beschränkung gilt lediglich dahingehend, dass vom Beschlagnahmeschutz nur Daten erfasst sind, die aus dem Gewahrsam des genannten Personenkreises stammen und einen ausreichenden Bezug zum Arzt-Patient-Verhältnis aufweisen.[58] Daten der Krankenversicherungen bzw. derer Verbände unterfallen dem Beschlagnahmeverbot beispielsweise nicht.

Die Problematik des Beschlagnahmeschutzes ist damit für Gesundheits-Clouds innerhalb und außerhalb der Gesundheits-Telematik befriedigend gelöst. Das gilt allerdings nur mit einer wesentlichen Einschränkung: Der Schutz des § 97 Abs. 2 Satz 2 StPO endet an den deutschen Grenzen. Sollen die Gesundheitsdaten also tatsächlich denselben Schutz genießen wie bei einer Speicherung durch Berufsgeheimnisträger, muss sowohl der Speicherort innerhalb Deutschlands liegen als auch sichergestellt sein, dass der Dienstleister (oder ggf. ihn beherrschende Muttergesellschaften) nicht ausländischen Offenbarungspflichten unterliegen.[59]

6 Fazit

Der Einsatz von Cloud Computing im Gesundheitssektor birgt wegen des Umgangs mit besonders sensiblen personenbezogenen Daten besondere Risiken, ist aber nach geltendem Recht nicht von vornherein ausgeschlossen, wenn die Vorgaben des Datenschutz-, Straf- und Sozialrechts strikt beachtet und in eine rechtskonforme Technikgestaltung umgesetzt werden. Zur Lösung der verbleibenden Probleme finden sich Ansätze in den Regelungen über die Telematik-Infrastruktur; dies gilt unabhängig davon, ob diese selbst Cloud Elemente aufweist. Während der Beschlagnahmeschutz bereits heute über die Telematik-Infrastruktur hinausgeht und Gesundheits-Clouds erfasst, ist die explizite Anordnung der Anwendung chipkartenbasierter Authentisierungsmechanismen auf die Telematik-Infrastruktur beschränkt. Hier ist eine gesetzliche Erweiterung auf den gesamten Gesundheitssektor zu erwägen.

Das größte Hindernis dürfte daneben die Unklarheit über das grundsätzliche Vorliegen einer Offenbarung i.S.d. § 203 Abs. 1 StGB bei Beauftragung externer Dienstleister sein. Sofern dieses Problem wegen der langen Aufbewahrungsfristen selbst durch den Einsatz von – derzeit – adäquaten Verschlüsselungsverfahren nicht vollständig beseitigt wird, kann auch hier nur der Gesetzgeber Abhilfe schaffen. Unabhängig davon ist mehr noch als bei anderen Anwendungen des Cloud Computings äußerste Zurückhaltung bei der – häufig Cloud-immanenten – Übermittlung von Daten einer Gesundheits-Cloud ins Ausland geboten, weil hierdurch u.a. der Beschlagnahmeschutz nicht mehr greift. An diesem Beispiel zeigen sich auch die Grenzen rein rechtlicher Schutzkonzepte, weshalb die Hoffnung auf die Erforschung rechtskonformer Optionen zur Technikgestaltung (v.a. im Bereich geeigneter Anonymisierungs- und Verschlüsselungskonzepte) liegen muss. Von deren Verfügbarkeit wird es nicht nur abhängen, ob Cloud Lösungen im Gesundheitswesen auch mit Blick auf die europäische Datenschutzreform eingesetzt werden dürfen.[60] Auch neue gesetzliche Ermächtigungsgrundlagen werden verfassungsrechtlich nur zulässig sein, wenn entsprechende technisch-organisatorische Schutzmechanismen verbindlich vorgeschrieben werden.

50 S. *Roßnagel/Hornung*, MedR 2008, 538 ff.; dort auch zum Vorschlag einer gesetzlichen Änderung.

51 Entsprechende Lösungen werden derzeit im Projekt SkIDentity erforscht, s. http://www.skidentity.com.

52 Dazu *Hornung*, (Fn. 5), 233 ff.

53 S. *Hornung* (Fn. 5), 235; *Dierks* (Fn. 45), 7.

54 Dafür *Hornung* (Fn. 5), 235; a.A. *Dierks* (Fn. 45), 17 f.

55 Unter den Begriff der Gegenstände fallen im Zusammenhang mit § 94 StPO („Beweisgegenstände"), auch Datenträger und v.a. digital gespeicherte Informationen, s. *Mayer-Goßner*, StGB, 55. A. 2012, § 94 Rn. 4, mit Verweis bzgl. Letzterem auf BVerfGE 124, 43.

56 Für einen entsprechend weiten Begriff des Dienstleisters auch *Dierks* (Fn. 45), 18.

57 S. die knappe Begründung, BT-Drs. 15/1525, 168; so auch *Dierks* (Fn. 45), 8.

58 S. *Dierks* (Fn. 45), 18.

59 Zur parallelen Diskussion im Datenschutzrecht s. Fn. 32.

60 S. zur Reform mit Blick auf das Cloud Computing *Hornung/Sädtler,* CR 2012, 683.