Marit Hansen

# Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter

Das Bundesverfassungsgericht hat 2008 im Urteil zur Online-Durchsuchung das Grundrecht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme postuliert. Welche Herausforderungen stellen sich vier Jahre später bei einem heute typischen Einsatz von IT-Systemen, dem Cloud Computing?

## 1 Einführung[1]

Das Bundesverfassungsgericht (BVerfG) spielt seit Jahrzehnten eine wichtige Rolle in Datenschutzfragen. Herausragend sind die beiden Urteile, in denen Datenschutz-Grundrechte aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleitet wurden: zum einen das Recht auf informationelle Selbstbestimmung, 1983 vom BVerfG im bekannten Volkszählungsurteil begründet [10], und zum anderen das Recht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme, das 2008 bei der Befassung mit den Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung herausgearbeitet wurde [11].

Unter „Cloud Computing" versteht man das Bereitstellen von Datenverarbeitungsressourcen (z.B. Prozessorleistung, Speicher, Netzwerkkapazitäten oder Software) durch Cloud-Anbieter für Anwender, die diese Ressourcen dynamisch und ohne Verzögerung anfordern und nutzen können. Nicht immer ist den Nutzern bewusst, wenn ihre Daten in einer Cloud verarbeitet werden, statt auf einem bestimmten Rechner an einem bestimmten Ort zu verbleiben. Im Folgenden geht es um Cloud Computing in der Form, dass die Datenverarbeitung in einer durch Dritte betriebenen Cloud erfolgt, die nicht unter der vollständigen Kontrolle des Anwenders steht.

Dieser Text ist wie folgt aufgebaut: Kapitel 2 erläutert die Schutzziele Vertraulichkeit und Integrität. Es untersucht zudem, inwieweit das BVerfG-Urteil von 2008 Cloud Computing umfasst. Kapitel 3 skizziert technische Möglichkeiten für Vertraulichkeit und Integrität, die überwiegend aus Forschungsprojekten stammen. Kapitel 4 zeigt beispielhaft, welchen rechtlichen Verpflichtungen ein Cloud-Anbieter mit Sitz im Ausland unterliegen kann. Schließlich fasst Kapitel 5 die Ergebnisse zusammen und gibt einen Ausblick.

1 Die dieser Publikation zugrundeliegende Arbeit wurde teilweise vom TClouds-Projekt (www.tclouds-project.eu/) unterstützt, das im 7. Forschungsrahmenprogramm der Europäischen Union gefördert wird (Grant Agreement No. ICT-257243).

**Marit Hansen**

Stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel

E-Mail: marit.hansen@datenschutzzentrum.de

## 2 Grundlagen

Vertraulichkeit und Integrität werden zu den Schutzzielen der Informationssicherheit gerechnet. Im Urteil des BVerfG von 2008 wird unter Vertraulichkeit der Schutz gegen ein Ausspähen vorhandener Daten und unter Integrität ein Schutz gegen das Manipulieren dieser Daten verstanden [11, Abs. 180]. Dies soll sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten umfassen [11, Abs. 205].

Im Folgenden ordnet Abschnitt 2.1 dieses Beitrags nun die Begriffe Vertraulichkeit und Integrität, wie vom BVerfG verwendet, in die jahrelange Debatte um Schutzziele ein. Abschnitt 2.2 greift wichtige Teile aus dem Urteil auf und diskutiert, inwieweit Cloud Computing vom Recht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systems erfasst ist. Die Ergebnisse stellt Abschnitt 2.3 in den Zusammenhang mit aktuellen Cloud-Trends.

### 2.1 Begriffe der Informationssicherheit

In den vergangenen Jahren hat die Diskussion um Schutzziele und die Arbeit mit ihnen eine größere Relevanz erreicht. Insbesondere wurden spezielle datenschutzspezifische Schutzziele in Ergänzung zu den klassischen drei Zielen der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – vorgeschla-

gen [33] und in jüngerer Zeit weiter ausgebaut. In einem Überblickspapier [2] betonen die Autoren, dass selbst etablierte Standardwerke die Schutzziele nicht konkret definieren, in jedem Fall aber kein vollständiger Konsens über die exakten Definitionen besteht. Eine Kategorisierung aus dem Jahr 2000 wählte weite Definitionen, um beispielsweise das gesamte Feld der Datensparsamkeit und Datenvermeidung in Kommunikationsnetzen unter „Vertraulichkeit" zu verorten [16] und damit leichter zugänglich für Informationssicherheitsbetrachtungen zu machen. Teile davon befinden sich in den Common Criteria, die mit einer eigenen „Privacy-Familie" Datensparsamkeitsanforderungen neben die klassischen Schutzziele stellt [14]. Auch für Integrität sind verschiedene Definitionen gängig – je nachdem, ob darunter ein vollständiger Schutz vor Manipulation oder nur deren Erkennbarkeit verstanden wird [16].

Das BVerfG-Urteil von 2008 greift auf die beiden mit dem Privatsphärenschutz am meisten verbundenen klassischen Schutzziele zurück: Vertraulichkeit und Integrität. Da es um einen Schutz gegen Missbrauch von vorhandenen (d.h. verfügbaren) Informationen geht, ist es berechtigt, sich auf diese Schutzziele zu konzentrieren. Verfügbarkeitsanforderungen etwa für Prozesse für die Wahrnehmung von Betroffenenrechten, die essentiell für Datenschutz sind, stehen in diesem Sinne außerhalb der Betrachtung.

Die Formulierung „Gewährleistung von Vertraulichkeit und Integrität" im BVerfG-Urteil darf allerdings nicht so (miss)verstanden werden, dass damit die in einigen Zusammenhängen gebotenen Datenschutzanforderungen nach gewissen Unschärfen („Kontingenz" [33]) im Gegensatz zu einer perfekten Integrität oder über die Vertraulichkeit hinausgehende Datensparsamkeitsansätze ausgeschlossen wären.

Als besondere Art der Integrität spielt die „kontextuelle Integrität" eine Rolle, die fordert, dass die Bindung von Informationen an einen Kontext erhalten bleibt. „Contextual Integrity" wurde 1998 als abstraktes Konzept für Privacy in die US-Diskussion eingebracht [28] und ist, nicht nur in Form der verwandten Zweckbindung, Bestandteil der europäischen Debatte [5]. Kontextuelle Integrität bedeutet u.a., dass in der Regulierung (Policy-Design oder Gesetzgebung) der jeweilige Kontext entscheidend für die Ausgestaltung ist. Technisch werden Ansätze diskutiert, um unmanipuliert relevante Kontextinformationen zu bestimmten Daten mitzuführen.

### 2.2 Anwendbarkeit des Urteils auf Cloud-Computing

Es überrascht nicht, dass sich das BVerfG-Urteil zur Online-Durchsuchung mit vernetzten PCs auf Nutzerseite und den rechtlichen Möglichkeiten einer Infiltration durch den Staat befasst. Jedoch sind die Richter in ihren Beratungen und im Urteilstext weit darüber hinausgegangen. Beispielsweise wird im Urteil explizit erwähnt, das Recht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme erstrecke sich auch „auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können" [11, Abs. 203].

Die Vernetzung, wie dies bei der Nutzung von Cloud Computing-Angeboten wesentlich ist, wird im Urteil besonders betont: „[...] führt die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation" [11, Abs. 179].

Wesentlich ist im Urteil, dass Betroffene unberechtigte Zugriffe kaum bemerken können: „Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren" [11, Abs. 180]. Genau dies ist in der Regel für fremdbetriebene Clouds gegeben.

Dennoch adressiert das Urteil primär das eigene IT-System – also zunächst nicht die Systeme einer Cloud: „Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt" [11, Abs. 206].

Das „Cloud-Zeitalter" deutete sich 2008 zwar schon am Horizont an, doch war noch wenig zu spüren von der heutigen Selbstverständlichkeit einiger Angebote, Cloud-Anwendungen zu integrieren (s.u.). In solchen Fällen geht der Betroffene normalerweise nicht davon aus, dass er außerhalb seines Schutzbereiches agiert. In diesem Sinn fährt Abs. 206 fort: „Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf."

### 2.3 Cloud-Durchdringung bei der eigenen Nutzung

Der Trend nicht nur bei Privatnutzern weg vom PC hin zu Tablet-Rechnern oder Smartphones verschiebt gleichzeitig die Nutzung vieler Datenverarbeitungsressourcen in die Cloud. Einige Programme, die vorher lokal abliefen, werden nun standardmäßig in der Cloud ausgeführt. Dies ermöglicht aufseiten des Nutzers, der auf seinem Tablet-Rechner oder Smartphone mit beschränkten Ressourcen auskommen muss, eine nahezu beliebige Erweiterung der Nutzungsarten, soweit die Internet-Verbindung schnell genug für den nötigen Datentransfer ist.

Dies betrifft beispielsweise Konvertierungsprogramme: Gerade bei proprietären Formaten einiger Anbieter ist es für eine Zusammenarbeit mit anderen erforderlich, die entstandenen Dateien umzuwandeln. Dies funktionierte früher lokal; jetzt ist vielfach die Cloud-Nutzung des (im Ausland ansässigen) Anbieters zum Standard geworden. Ähnliches geschieht bei den Sprachassistenzsystemen der Smartphones (z.B. Siri von Apple), die ohne Online-Nutzung einer Cloud deutlich weniger leistungsfähig wären. Durch solche Dienste werden sehr viele Informationen standardmäßig über ausländische Server geleitet, und aufgrund der Dienstgestaltung wäre eine verschlüsselte Verarbeitung – geschützt gegen mögliche Zugriffe durch den Anbieter – in diesen Fällen nicht möglich.

Hier mischen sich Clouds und persönlich genutzte informationstechnische Systeme – also müsste für diese Fälle das Recht auf Gewährleistung von Vertraulichkeit und Integrität informa-

tionstechnischer Systeme gelten. Inwieweit dies technisch bzw. rechtlich gegeben ist, beschreiben die nächsten beiden Kapitel.

## 3 Vertraulichkeit und Integrität – die technische Perspektive

Aus technischer Sicht sind die Maßnahmen entscheidend, die Vertraulichkeit und Integrität sicherstellen oder zumindest unterstützen können. Wo ein umfassendes Sicherstellen eines Schutzziels nicht möglich ist, können technische oder organisatorische Maßnahmen vorgesehen werden, die eine Verletzung des Schutzziels erkennbar macht [16]. Beispielsweise hilft eine Protokollierung von Aktionen, unberechtigte lesende oder ändernde Zugriffe festzustellen und aufzuklären, was wiederum Abschreckungswirkung haben kann.

Die Basis für technische und organisatorische Maßnahmen sollten generelle Vertrauenswürdigkeitsbelege der Cloud-Anbieter bilden, z.B. durch Transparenz über Funktionsweisen und Risiken, Belege zur Qualifikation des Personals, anerkannte Zertifizierungen oder aussagekräftige Security Service Level Agreements [9][29]. Der aktuelle Stand und Entwicklungen in Bezug auf Maßnahmen zur Vertraulichkeit (s. Abschnitt 3.1) und zur Integrität (s. Abschnitt 3.2) werden im Folgenden beschrieben.

### 3.1 Vertraulichkeit: Schutz vor Kenntnisnahme

Während die Datenübertragung zwischen Anwender und Cloud-Anbieter häufig verschlüsselt abläuft (z.B. per SSL), ist dies bei Datenspeicherung und sonstiger Verarbeitung zumeist nicht der Fall. Für die verschlüsselte Datenspeicherung gibt es vielfältige Ansätze. Nicht immer steht der Verschlüsselungsschlüssel dabei unter der Kontrolle des Anwenders, und sehr häufig wird Cloud-seitig entschlüsselt, wobei die Daten zumindest temporär im Hauptspeicher, ggf. aber sogar ausgelagert auf Festplatten, gespeichert sind.

Im besten Fall liegen auf den fremden Rechnern in der Cloud nie entschlüsselte Daten der Anwender vor. Dies ist beispielsweise dann möglich, wenn nur auf den Endgeräten der Anwender ent- und verschlüsselt wird [30], z.B. in Kombination mit Hardware Security Modules [26]. Daneben wird intensiv an homomorpher Verschlüsselung geforscht, die für gewisse mathematische Operationen eine Verarbeitung der Daten in verschlüsseltem Zustand erlaubt. Für eine vollumfassende Datenverarbeitung sind die Verfahren (noch) nicht ausreichend performant [24].

Generell müssen bei Kryptoverfahren Schutzniveau und Risiken immer wieder neu bewertet werden [34] – Schlüssellängen müssen angepasst, Verfahren ausgetauscht werden [7]. Dass der Schutz brüchig werden kann, muss man nicht erst bei einer Langzeitspeicherung berücksichtigen, sondern schon dann, wenn sensible Daten den eigenen Kontrollbereich verlassen.

Neben manipulationsfesten Systemen („Tamperproof Hardware“) bietet die Fragmentierung der Informationen und die Verteilung auf mehrere Clouds (mit unterschiedlichen Eigenschaften) einen weiteren Lösungsansatz. Beispielsweise kann man sensiblere Daten in einer vertrauenswürdigen Private Cloud und die übrigen in einer Public Cloud verarbeiten lassen [8][23]. Solche Fragmentierungen sind auch in größerem Maßstab möglich, indem beispielsweise Informationen wie Datenbankeinträge auf verschiedene Clouds mit verschiedenen Schlüsseln verschlüsselt abgelegt und ggf. getrennt verarbeitet werden [21]. Wegen der vielfältigen Anforderungen der Anwender werden künftig mehr Lösungen diskutiert werden, die mehrere, ggf. miteinander verknüpfte Clouds integrieren [18]. Hier gilt es, den Anwenderbedingungen durch eine geeignete Kombination von Clouds mit den passenden Sicherheitsgarantien gerecht zu werden.

Selbst wenn für Anbieter die Inhalte der Daten in der Cloud nicht im Klartext sichtbar sind, können sie zumeist feststellen, wann welche Nutzer aktiv sind und teilweise auch erkennen, welche Aktionen sie durchführen. Aus anderen Internetbereichen bekannte Anonymisierungstechniken, beispielsweise durch Einbindung von Proxies oder Dummy Traffic, können hier Abhilfe schaffen [36][39].

Zu den Vertraulichkeitsanforderungen gehört es, dass zu löschende Daten tatsächlich rückstandsfrei entfernt werden. Dies wird von vielen Cloud-Angeboten gegenwärtig nicht gewährleistet.

### 3.2 Integrität: Schutz vor (unentdeckbarer) Manipulation

Auch für den Schutz vor Manipulation von Daten sind kryptographische Verfahren, wie in Abschnitt 3.1 erwähnt, hilfreich. Daneben können Prüfsummen oder Signaturen über die Dateien mitgespeichert werden, um Veränderungen aufdeckbar zu machen. In dem Fall müssten die korrekten Daten aus vertrauenswürdiger Quelle wiederhergestellt werden. Dies kann z.B. durch die Verwendung mehrerer Clouds für die Daten geschehen (z.B. [3][2]).

Von erheblichem Interesse für die Integrität der Daten sind die Schnittstellen für die Cloud-Verwaltung. Manipulationen auf dieser Ebene können einem Angreifer den Vollzugriff über Kundenaccounts und die gespeicherten Daten verschaffen. Für eine Vielzahl möglicher Angriffe sind bereits Gegenmaßnahmen vorgeschlagen und auch teilweise von Cloud-Anbietern implementiert worden [35]. Jedoch kann in diesem Punkt keine Entwarnung gegeben werden.

Eine weitere Maßnahme besteht in der Protokollierung aller Aktionen, die relevant für die Daten oder den Account der Anwender sein können. Dies betrifft insbesondere die Administratoren aufseiten der Cloud-Anbieter. Jeder Anwender muss die für ihn wesentlichen Protokollierungsdaten einsehen können; hier ist – wie auch bei den Accounts selbst – eine Mandantentrennung vorzusehen, so dass andere Anwender keine Erkenntnisse über die eigenen Daten erlangen können. Gleichzeitig gelten hohe Integritätsanforderungen an die Protokollierung, die revisionssicher sein muss [1].[3] Auch sollten Anwender in Echtzeit auf solche Protokollierungsdaten zugreifen können [15].

Weitergehende Forderungen beinhalten sogar ein in die Cloud integriertes „Risk Assessment as a Service“, weil die herkömmlichen Ansätze an Grenzen stoßen [22]. Bislang sind Ansätze einer möglichst automatisierten Prüfung von sicherheitsrelevanten Eigenschaften [13] noch nicht ausgereift. Bei Sicherheitsvorfällen benötigen Ermittler weitere Informationen, um den Sachverhalt exakt aufklären zu können. Für die möglichen forensischen Detailanalysen fehlen aufgrund der Vielfalt der Cloud-Angebote bislang Standards [4].

2 Allerdings sind die Ergebnisse nicht auf Infrastructure-as-a-Service mit dem Angebot virtueller Maschinen übertragbar [32].

3 Im Übrigen gelten die Datensparsamkeitsanforderungen auch für Protokollierungsdaten [1].

Ein weiteres Instrument für Integritätssicherung, das für einige Einsatzbereiche prototypisch implementiert ist, besteht in der Verwendung von Trusted Computing (z.B. [27]). Diese Technik kann auch verwendet werden, wenn die Verarbeitungsregeln (Policy) unmittelbar mit den gespeicherten Daten verknüpft abgelegt werden.[4] Zu diesem Zweck werden die Daten verschlüsselt gespeichert. Bei jedem Zugriff wird zunächst die angehängte Policy ausgewertet, die darüber entscheidet, ob die gewünschte Verarbeitung durch den ausführenden Nutzer erlaubt wird oder nicht. Mit diesem Mechanismus ließen sich ebenfalls die nötigen Informationen für eine kontextuelle Integrität mitführen.

In diesem Zusammenhang wäre es sinnvoll, wenn standardmäßig Datenverarbeitungsorte und –verantwortliche direkt bei der Verarbeitung erkennbar wären und automatisiert ausgewertet und gesteuert werden könnten. Ein Anwender könnte z.B. konfigurieren, dass personenbezogene Daten bestimmte Regionen (wie den Europäischen Wirtschaftsraum (EWR)) nie verlassen, andere – weniger sensible – Daten aber durchaus anderswo verarbeitet werden dürften. Gerade für Cloud-of-Cloud-Ansätze sollten Eigenschaften der verschiedenen Cloud-Angebote automatisiert auswertbar sein.

## 4 Vertraulichkeit und Integrität – die rechtliche Perspektive

Das Rechtsregime, in dem sich der Cloud-Anbieter befindet oder seinen Sitz hat, ist entscheidend dafür, welche juristischen Zugriffs- und Auswertungsbefugnisse bestehen. Da viele Cloud-Anbieter ihren Sitz außerhalb von Deutschland haben, sind die dortigen Zugriffsbefugnisse relevant – zur Kenntnisnahme (s. Abschnitt 4.1) oder sogar für ändernde Eingriffe (s. Abschnitt 4.2).

### 4.1 Kenntnisnahme

Vielfach haben bestimmte Behörden das Recht, auf bei Anbietern gespeicherte Daten lesend zuzugreifen. Die meisten Rechtsgrundlagen dafür stammen aus dem Bereich der polizeilichen Strafverfolgung und der nationalen Sicherheit; allerdings bestehen teilweise auch Zugriffsbefugnisse aus Gründen des Urheberrechts.

Im Jahr 2008 wurde über Befürchtungen von Geheimdiensten und Militärs der USA berichtet, dass sie quasi „blind" für viele Entwicklungen würden, weil ein Großteil des Internet-Verkehrs nicht mehr wie früher über die USA geleitet wird [25]. Während 1998 noch ca. 70% des weltweiten Internet-Verkehrs über die USA geroutet wurde, hat sich dieser Anteil mittlerweile auf etwa 25% verringert. Dies könnte ein Grund dafür sein, dass die USA in letzter Zeit weitere rechtliche Regelungen eingeführt haben, die ihnen einen Zugriff auf Daten auch außerhalb ihres Landes einräumen.

Mitte 2011 wurde öffentlich, dass mit der rechtlichen Begründung „Patriot Act" nicht nur auf Cloud-Daten zugegriffen werden darf, die in den USA verarbeitet werden, sondern auch auf Daten, die ausschließlich auf europäischen Servern liegen, sofern der Cloud-Anbieter seinen Sitz in den USA hat [38]. Dies gilt selbst für rechtlich selbstständige Tochterunternehmen. Vorher waren viele davon ausgegangen, dass Daten, die rein innereuropäisch verarbeitet werden, d.h. die EU und den EWR nie verlassen, gegen Zugriffe von außerhalb geschützt wären.

Neben dem Patriot Act kommen weitere Rechtsgrundlagen für eine Beschlagnahme solcher Daten zur Anwendung (ausführlicher beschrieben in [37]). Für Ermittlungen im Bereich der Steuer-, Finanz-, Wirtschafts-, Drogen- und Organisierter Kriminalität können Anordnungen auf einer „Bank of Nova Scotia Subpoena" beruhen. In Bezug auf Angaben zu Bankkonten können sog. erzwungene Einwilligungsanordnungen („Compelled Consent Order") verhängt werden.

Eine spezielle Berücksichtigung von Clouds, für die Zugriffe aus den USA erlaubt werden, findet sich im Foreign Intelligence Surveillance Act (FISA) mit dem Amendment 1881 aus dem Jahre 2008 [6]. Mit dem Ziel, Nicht-US-Bürger außerhalb den USA zu beobachten („targeting certain persons outside the United States"), sind „Remote Computing Services" – dies umfasst Clouds – gesondert erwähnt.

Viele dieser Zugriffsbefugnisse erfordern einen richterlichen Beschluss o.ä. Jedoch wurden Fälle bekannt, in denen das FBI an Provider einen „National Security Letter" mit Zugriffsbitten verschickt hat. Dass diese „Bitten" zu erfüllen sind, berichtet der Provider Nick Merrill, der sechs Jahre lang wegen einer sog. „Gagging Order" (ein verhängter Maulkorb) darüber nicht frei sprechen durfte [19].

Speichert der Anbieter die Daten verschlüsselt, bedeutet dies nicht, dass sie vor seinen Zugriffen geschützt sind. So kann Apple trotz verschlüsselter Speicherung in der angebotenen iCloud auf die Kundendaten im Klartext zugreifen [17] – die Kontrolle über die Schlüssel verbleibt bei „Software as a Service"-Angeboten beim Anbieter.

Ähnliche Beispiele für Zugriffsbefugnisse auf die gespeicherten Daten bestehen in weiteren Ländern mit einer Überwachungstradition wie China oder in arabischen Staaten [31]. Es ist weder für die Betroffenen noch für Deutschland oder Europa kontrollierbar, zu welchen Zwecken welche privaten Daten von Personen oder Geschäftsgeheimnisse ausgewertet werden und welche Folgen dies hat.

Staatliche Zugriffsbefugnisse sind dann problematisch, wenn die Voraussetzungen für das Lesen und Auswerten der Daten nicht klar definiert oder zu niedrigschwellig sind, die Befugnisse zu weit gehen, Betroffene nicht über Zugriffe informiert werden (auch nicht im Nachhinein) und für sie kein effektiver Rechtsschutz besteht.

Übrigens haben auch einige EU-Länder weitgehende Zugriffsermächtigungen, die vielen Nutzern in Deutschland unbekannt sind. Dies wirft die Frage auf, inwieweit ein (rechtlich zulässiger) Transfer personenbezogener Daten innerhalb des EWR faktisch problematisch sein kann, wenn Behörden in den Exportländern zu weitreichende Zugriffsbefugnisse haben. Ein Beispiel ist der britische Regulation of Investigatory Powers Act (RIPA) aus dem Jahre 2000, der beispielsweise bei Androhung von Haftstrafen dazu verpflichtet, Kryptoschlüssel herauszugeben [6].

In Schweden erlaubt das FRA-Gesetz (Proposition 2006/07:63 – En anpassad försvarsunderrättelseverksamhet) eine umfassende Überwachung der Telekommunikation von Nicht-Schweden: FRA ist die Abkürzung für die schwedische geheimdienstlich tätige Behörde „Försvarets radioanstalt", die dem Verteidigungsminister untersteht. Das FRA-Gesetz ist seit Anfang 2009 in Kraft und erlaubt es der FRA-Behörde, anlasslos und ohne richterlichen

4 In [12] als „Information-Centric Security" bezeichnet; verwandt ist das Konzept der „Sticky Policies".

Beschluss alle Telefon- und Internet-Kommunikation abzuhören bzw. mitzulesen. Daraus gewonnene Informationen können an weitere Staaten weitergegeben werden.

Wann immer schützenswerte Daten in einer Cloud verarbeitet werden sollen, muss die stets durchzuführende Risikoanalyse rechtliche Zugriffsbefugnisse einbeziehen. Aus diesem Grund ist es nötig, dass der Anwender über sämtliche mögliche Verarbeitungsorte informiert wird [1].

### 4.2 Eingriffe

Neben dem lesenden Zugriff behalten sich Cloud-Anbieter oder staatliche Stellen in einigen Ländern vor, im Rahmen von Inhaltskontrollen, z.B. zum Durchsetzen von Moralvorstellungen, Dateien zu ändern oder zu löschen.

Bekannt wurde der Fall eines deutschen Hobbyfotografen, der künstlerische Teilaktbilder in seinem nicht öffentlich zugänglichen Backup in einer Cloud speicherte. Ihm wurde – zunächst ohne Begründung – der Zugang gesperrt. Nach seiner Beschwerde erhielt er nach einigen Tagen eine E-Mail, er habe gegen die Nutzungsbedingungen verstoßen – wegen „Nacktheit“ [20]. Ein Rechtsverstoß wurde ihm nicht angelastet.

Tatsächlich findet man in vielen Nutzungsbedingungen („Terms and Conditions“) – besonders für die Nutzung durch Privatpersonen – Aussagen, dass der Cloud-Anbieter sich vorbehält, auf die gespeicherten Daten zuzugreifen und sie zu löschen oder zu verändern oder den Account zu sperren, wenn der Eindruck entsteht, dass damit Regelungen oder Moralvorstellungen verletzt werden. Beispielhaft werden dabei Inhalte angeführt, die als gotteslästerlich, obszön oder anstößig („profane, obscene, indecent“) empfunden werden könnten. Dabei ist es nicht unbedingt erforderlich, dass die gespeicherten Daten tatsächlich für andere Nutzer zugreifbar sind – auch ein Backup in einem persönlichen Bereich des Nutzers könnte in den Fokus geraten.

Für den Nutzer ist angesichts der unbestimmten Begriffe nicht vorhersehbar, wann ein derartiger „Anstößigkeitstatbestand“ erfüllt ist. In jedem Fall besteht das Risiko, dass ohne Ankündigung die Daten oder die zugehörigen Accounts blockiert oder gelöscht werden.

## 5 Zusammenfassung und Ausblick

Seit einigen Jahren führen Wissenschaftler einen intensiven Diskurs zu vielfältigen Lösungen, die Vertraulichkeit und Integrität bei Cloud Computing unterstützen. Jedoch findet man erst wenige dieser Ansätze in der Praxis.

Während sich im technischen Bereich das Niveau an Vertraulichkeit und Integrität tendenziell verbessert, erweitern einzelne Nationen ihre Zugriffsbefugnisse auf die in Clouds gespeicherten Daten, die sie dann über bestimmte Behörden und die Cloud-Anbieter ausüben können. Dies müssen Anwender bei der Auswahl von Cloud-Anbietern berücksichtigen und entsprechende Sicherheitsmaßnahmen vorsehen.

Problematisch ist es, dass für Geräte wie Tablet-Rechner oder Smartphones vielfach bestimmte Funktionalität nur noch in der Cloud des Service-Anbieters nutzbar ist. Für Dienste wie Sprachassistenz oder Formatkonvertierung sind die diskutierten Lösungsansätze für Vertraulichkeit der Informationen kaum nutzbar. Obwohl es sich primär um eigengenutzte IT-Systeme handelt, die sich mit Clouds verbinden, ist eine Anwendung und Durchsetzbarkeit des Rechts auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme insbesondere bei den ausländischen Marktführern schwierig. Allerdings sollte der Staat seinen Bürgern und den Unternehmen die Nutzungsrisiken bewusst und verständlich machen sowie risikoärmere und datenschutzrechtlich einwandfreie Alternativen fördern.

## Literatur


[1] AK Technik und AK Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2011) Orientierungshilfe – Cloud Computing. Version 1.0, Stand 26.09.2011, www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

[2] Bedner, M. / Ackermann, T. (2010) Schutzziele der IT-Sicherheit. DuD 34(5):323-328

[3] Bessani, A. et al. (2011) DepSky: Dependable and Secure Storage in a Cloud-of-Clouds. 6th ACM SIGOPS/EuroSys European Systems Conference (EuroSys '11), S. 31-45

[4] Birk, D. / Wegener, C. (2011) Technical Issues of Forensic Investigations in Cloud Computing Environments. IEEE 6th Int. Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), S. 1-10

[5] Borcea-Pfitzmann, K. / Pfitzmann, A. / Berg, M. (2011) Privacy 3.0 := data minimization + user control + contextual integrity. it – Information Technology 53(1):34-40

[6] Bowden, C. (2011) Privacy and surveillance on the Internet – What happened, and what to expect next… Präsentation vom 20.09.2011, http://wolnyinternet.panoptykon.org/sites/default/files/internet_surveillance_caspar_bowden.pdf

[7] Buchmann, J. / May, A. / Vollmer, U. (2006) Perspectives for Cryptographic Long-Term Security. CACM 49(9): 50-56

[8] Bugiel, S. et al. (2011) Twin Clouds: An Architecture for Secure Cloud Computing. Workshop on Cryptography and Security in Clouds (CSC'11), www.hgi.rub.de/hgi/publikationen/SSBN11/

[9] BSI (2011) Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter. 10.05.2011, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf

[10] BVerfG (1983) Urteil vom 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83

[11] BVerfG (2008) Urteil vom 27.02.2008, 1 BvR 370/07, Abs. 1-333

[12] Chow, R. et al. (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. 2009 ACM Workshop on Cloud Computing Security (CCSW '09), S. 85-90

[13] Cloud Security Alliance (2010) CloudAudit: Automated Audit, Assertion, Assessment, and Assurance. http://cloudaudit.org/CloudAudit/Downloads.html

[14] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 2.1 (1999) CCIMB-99-032, ISO/IEC 15408:1999, www.commoncriteriaportal.org/files/ccfiles/ccpart2v21.pdf

[15] Curry, Sam et al. (2010) Infrastructure Security: Getting to the Bottom of Compliance in the Cloud. RSA Security Brief, March 2010

[16] Federrath, H. / Pfitzmann, A. (2000) Gliederung und Systematisierung von Schutzzielen in IT-Systemen. DuD 24(12):704-710

[17] Foresman, C. (2012) Apple holds the master decryption key when it comes to iCloud security, privacy. Ars technica, 03.04.2012, http://arstechnica.com/apple/news/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy.ars

[18] Glott, Rüdiger et al. (2011) Trustworthy Clouds underpinning the Future Internet. In: Future Internet Assembly, LNCS 6656, Springer, S. 209-221

[19] Goodman, A. (2010) Gagged for 6 Years, Nick Merrill Speaks Out on Landmark Court Struggle Against FBI's National Security Letters. Interview, Democracy Now!, 11.08.2010, www.democracynow.org/2010/8/11/gagged_for_6_years_nick_merrill

[20] Heckert, M. (2011) Wie ein Handy-Fan von Wolke Sieben fiel. Aachener Zeitung vom 01.02.2011, www.az-web.de/sixcms/detail.php?template=az_detail&id=1533902
[21] Hudic, A. et al. (2012) Data Confidentiality using Fragmentation in Cloud Computing. Int. J. Communication Networks and Distributed Systems 1(3/4)
[22] Kaliski, B.S. / Pauley, W. (2010) Toward Risk Assessment as a Service in Cloud Environments. 2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '10)
[23] Ko, S.Y. / Jeon, K. / Morales, R. (2011) The HybrEx Model for Confidentiality and Privacy in Cloud Computing. 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11)
[24] Lauter, K. / Naehrig, M. / Vaikuntanathan, V. (2011) Can Homomorphic Encryption be Practical? 3rd ACM Workshop on Cloud Computing Security (CCSW'11)
[25] Markoff, J. (2008): Internet Traffic Begins to Bypass the U.S. The New York Times, 30.08.2008, www.nytimes.com/2008/08/30/business/30pipes.html
[26] Meyer, C. et al. (2011) *Sec²* – Ein mobiles Nutzer-kontrolliertes Sicherheitskonzept für Cloud-Storage. D.A.CH Security 2011, S. 285-295
[27] Neisse, R. / Holling, D. / Pretschner, A. (2011) Implementing Trust in Cloud Infrastructures. 2011 11th IEEE / ACM Int. Symposium on Cluster, Cloud and Grid Computing (CCGRID '11)
[28] Nissenbaum, H. (1998) Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy 17(5):559-596
[29] Paulus, S. (2011) Standards für Trusted Clouds – Anforderungen an Standards und aktuelle Entwicklungen. DuD 35(5):317-321
[30] Puttaswamy, K.P.N. / Kruegel, C. / Zhao, B.Y. (2011) Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications. 2nd ACM Symposium on Cloud Computing (SOCC '11)
[31] Rath, M. / Rothe, B. (2012) Vorsicht vor Clouds im Ausland. Computerwoche, 07.02.2012, www.computerwoche.de/2504448
[32] Rocha, F. / Correia, M. (2011) Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud. 1st Int. Workshop on Dependability of Cloud, Data Centers and Virtual Computing Environments (DCDV)
[33] Rost, M. / Pfitzmann, A. (2009) Datenschutz-Schutzziele – revisited. DuD 33(6):353-358
[34] Smart, N. (Hrsg.) (2011) ECRYPT II Yearly Report on Algorithms and Keysizes (2010-2011), www.ecrypt.eu.org/documents/D.SPA.17.pdf
[35] Somorovsky, J. (2011) All your clouds are belong to us: Security analysis of cloud management interfaces. 3rd ACM Workshop on Cloud Computing Security (CCSW '11)
[36] Strauch, S. et al. (2012) Cloud Data Patterns for Confidentiality. 2nd Int. Conference on Cloud Computing and Service Science (CLOSER 2012)
[37] ULD (2011) Inanspruchnahme des Patriot Acts und anderer US-rechtlicher Regelungen zur Beschaffung von personenbezogenen Daten aus dem Raum der Europäischen Union durch US-Behörden. Positionspapier, 15.11.2011, www.datenschutzzentrum.de/internationales/20111115-patriot-act.html
[38] Whittaker, Z. (2011) Microsoft admits Patriot Act can access EU-based cloud data. ZDNet, 28.06.2011, www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225
[39] Yau, S.S. / An, H.G. (2010) Confidentiality Protection in Cloud Computing Systems. Int. J. Software and Informatics 4(4):351-365