Cloud Storage-Services als Herausforderung für Strafverfolgungs- und Sicherheitsbehörden

Thomas Süptitz, Johannes Gorgus, Torsten Eymann

Universität Bayreuth
Lehrstuhl für Wirtschaftsinformatik
Universitätsstraße 30
95447 Bayreuth
Thomas.Sueptitz@bmf.bund.de
Johannes.Gorgus@uni-ulm.de
Torsten.Eymann@uni-bayreuth.de

Abstract: Cloud Storage-Dienste wie Dropbox, Skydrive & Co. erfreuen sich zunehmender Beliebtheit. Die Service-Provider speichern dabei die Daten regelmäßig auch auf ausländischen Servern. Dies hingegen wirft rechtliche Fragen auf, sobald deutsche Ermittlungsbehörden gerichtsverwertbar („legal“) auf diese Informationen zurückgreifen möchten. Um herauszufinden, ob mit der praktischen Arbeit der Strafverfolger tatsächlich Schwierigkeiten einhergehen, haben wir eine qualitative Studie durchgeführt. Dafür konnten wir insgesamt sieben Wissenschaftler, Staatsanwälte und Richter sowie einen Bundespolitiker befragen. Die Resultate bestätigen die Probleme und zeigen zugleich die Vielschichtigkeit der Thematik auf.

1 Einleitung

Anfang Juni 2013 wurden die ersten Enthüllungen des bis dahin anonymen Whistleblowers Edward Snowden über Spionage- und Überwachungsmaßnahmen diverser Geheimdienste in den Medien veröffentlicht Die Skandale über diese globale Internetüberwachung täuschen allerdings darüber hinweg, dass der „legale“ Zugriff auf Dateien bei Cloud Storage-Dienstleistern für deutsche Strafverfolger mit erheblichen Schwierigkeiten verbunden sein kann. Besondere Bedeutung erhält diese Frage, wenn man die wachsende Nutzung der Online-Speicherdienste im Kontext des zunehmenden Speicherbedarfs der Nutzer betrachtet [GI13]. Zudem können die Angebote für Täter einen Anreiz bieten, den Ermittlungsbehörden Beweismittel bewusst vorzuenthalten.

Im zweiten Kapitel werden wir deshalb die technischen Grundlagen des Cloud Storage, die aktuelle Gesetzgebung sowie verwandte Arbeiten diskutieren. Mit unserer Arbeit verfolgen wir das Ziel, folgende Fragen zu beantworten: (a) Ergeben sich durch die gegenwärtige Gesetzeslage in Deutschland Komplikationen für Ermittlungsbehörden; und zwar derart, dass auf Beweismittel, die bei Cloud Storage-Betreibern gespeichert wurden, nur schwerlich oder gar nicht zugegriffen werden kann?, (b) Inwiefern sind diese Situationen herausfordernd?, (c) Wie wird diesen Schwierigkeiten bei der täglichen

Arbeit begegnet; werden pragmatische „Work-Arounds“ entwickelt?, (d) Existiert bei den Strafverfolgern ein Bewusstsein oder ein Verständnis für die Problematik?

Die Methodik zur Beantwortung dieser Fragen wird im dritten Kapitel besprochen, während im vierten Kapitel die Ergebnisse unserer qualitativen Studie diskutiert und ausgewertet werden. Die Erkenntnisse werden abschließend zusammengefasst und gewürdigt (fünftes Kapitel).

2 Technische und strafprozessuale Problemstellung

Die zu untersuchende Problematik ist Folge der technischen Abläufe bei Cloud Speicherdiensten und deren Architektur sowie der deutschen Gesetzgebung. Insofern überrascht es nicht, dass die Thematik – ausschließlich - in der juristischen Literatur diskutiert wird.[1] Zuvor widmen wir uns jedoch den zugrundliegenden technischen Aspekten.

2.1 Wesensmerkmale des Cloud Computing und von Cloud Storage

Obwohl eine einheitliche Definition des Begriffs „Cloud Computing“ bislang fehlt, ist die Begriffsbestimmung des National Institutes of Standards and Technology (NIST) sehr weit verbreitet. Danach umschreibt der Begriff die über ein Netzwerk erfolgende Bereitstellung eines mit weiteren Nutzern geteilten Pools von IT-Ressourcen. Dabei kann es sich um Server, Speicher, Netzwerke oder Applikationen handeln. Auf die Services kann ohne großen Aufwand zugegriffen werden, während die nötigen Kapazitäten flexibel je nach Bedarf des Kunden angepasst werden können [RPZ10].

Der Anbieter der Services, der Cloud Service-Provider, stellt mithilfe eigener oder von Subunternehmern betriebenen Rechenzentren die erforderliche Infrastruktur zur Verfügung. Diese sind in der Regel auf verschiedene Orte verteilt [BW10].

Cloud Computing zeichnet sich vor allem durch die Skalierbarkeit und die Flexibilität der benötigten IT-Ressourcen aus [SR09]. Die verfügbaren IT-Ressourcen werden mittels einer Virtualisierungsebene (Virtual Machine Monitor/Hypervisor) von der konkreten physikalischen Recheneinheit abstrahiert, zusammengeführt und für die Nutzung durch mehrere Anwender verwaltet [HW10]. Hat ein Kunde entsprechenden Bedarf, wird diesem die benötigte Ressource im gewünschten Umfang aus dem Pool bereitgestellt. Sollte die Ressource in diesem Umfang nicht mehr gebraucht werden, wird diese dynamisch zurückgezogen und anderen Kunden zur Verfügung gestellt [PA09]. Aufgrund dieser permanenten Neuzuweisung der Kapazitäten an verschiedene Kunden ist eine Zuordnung zu einer bestimmten physikalischen Recheneinheit nicht möglich [SR09].

[1] Für einen umfassenden Überblick über die überaus umfangreiche juristische Dimension sei auf [Bä11], [Ge09a] und [SUE13] verwiesen.

2.2 Strafprozessuale Problemstellung

Im Rahmen eines Strafverfahrens müssen die Strafverfolger versuchen, die Schuld oder Unschuld eines Täters zu beweisen. Dafür eröffnet die Strafprozessordnung (StPO) eine Vielzahl von Maßnahmen. Dazu zählt u.a. die Möglichkeit, Wohnungen und andere Räume zu durchsuchen. Ist der Beschuldigte selbst von der Durchsuchung betroffen, so gestattet dies § 102 StPO. Für die Durchsuchung bei anderen Personen ist hingegen § 103 StPO einschlägig. Da mit einer solchen Durchsuchung ein erheblicher Grundrechtseingriff verbunden ist, ist regelmäßig ein richterlicher Durchsuchungsbeschluss notwendig. Dieser ermöglicht auch die Inbetriebnahme vorgefundener EDV-Anlagen [Bä11]. Die Untersuchung, ob die EDV-Anlage potentiell beweiserhebliche Daten aufweist, erlaubt § 110 StPO [AC11]. Diese Durchsicht eröffnet es den Ermittlern, über die Sicherstellung oder Beschlagnahme gemäß §§ 94 ff. StPO des Entdeckten zu entscheiden.[2] Mithin ergibt sich ein Dreiklang aus (I) Durchsuchung, (II) Durchsicht und (III) Sicherstellung/Beschlagnahme. Dabei ging der Gesetzgeber davon aus, dass nur körperliche Gegenstände einer amtlichen Verwahrung zugeführt werden können [OB10]. Demnach müsste die gesamte Hardware – und nicht nur die darauf befindlichen Daten – sichergestellt oder beschlagnahmt werden [GB09]. Da eine solche Maßnahme vielfach unverhältnismäßig sein dürfte, wird die Anfertigung von Kopien als milderes Mittel angesehen [AC11]. Nutzt der Anwender Dropbox, Skydrive & Co. in der Form, dass ein (gleichnamiger) Ordner auf dem lokalen Endgerät die Beweismittel enthält, kann folglich das Endgerät sichergestellt oder beschlagnahmt werden oder eine Kopie davon angefertigt werden.

2.2.1 Zugriff auf Daten in der Cloud

Rechtliche Besonderheiten ergeben sich dann, wenn Daten untersucht und in amtliche Verwahrung genommen werden sollen, die sich „in der Wolke“ befinden. Für den Rückgriff auf diese Daten bestehen prinzipiell zwei Ermittlungsansätze: der mittelbare Zugriff vom Endgerät des von der Haussuchung Betroffenen oder der unmittelbare Zugriff beim Cloud Service-Provider. Seitdem § 110 Abs. 3 StPO zum 21. Dezember 2007 eingeführt wurde, ist es möglich, auf einen externen Datenbestand zuzugreifen, der sich außerhalb des Durchsuchungsobjekts befindet [Sc08]. Die Cloud Service-Anbieter verfügen dabei über eine Vielzahl von Rechenzentren, die europa- oder gar weltweit verstreut sind [Ge10]. Dies führt regelmäßig dazu, dass ein Ermittler durch seinen mittelbaren Zugriff fremde Hoheitsrechte und somit das völkerrechtliche Souveränitätsprinzip [Ge09a] eines anderen Staates verletzt. Eine solche Transborder Search [SA08] wird durch § 110 Abs. 3 StPO allerdings gar nicht ermöglicht [Bä11].

Grundsätzlich kann natürlich auch der Cloud Service-Provider unmittelbar durchsucht werden. Diese Durchsuchung bei einem solchen Nichtverdächtigen gestattet § 103 StPO. Allerdings erweist sich auch hier das völkerrechtliche Souveränitätsprinzip als „hinder-

[2] Die Sicherstellung bzw. Beschlagnahme haben das Ziel den Übergang der Sachherrschaft auf den Staat zu ermöglichen. Erfolgt dieser einvernehmlich, spricht man von einer Sicherstellung; die zwangsweise Herstellung der amtlichen Verwahrung wird als Beschlagnahme bezeichnet.

lich“, sofern die Durchsuchungsmaßnahme im Ausland vorgenommen werden muss.[3] Zudem stellt sich eine praktische Herausforderung: Der physische Speicherort der Daten muss bestimmt werden können. Allerdings kann sich dieser stetig ändern.

2.2.2 Zugriff im Rahmen der Telekommunikationsüberwachung

Der zwischen dem Nutzer und dem Cloud Service-Provider fließende Datenverkehr könnte prinzipiell durch eine Ermittlungsbehörde abgefangen und ausgewertet werden. Diese Möglichkeit eröffnen die §§ 100a ff. StPO; die sog. Telekommunikationsüberwachung (TKÜ). Allerdings sind die daran geknüpften Bedingungen sehr restriktiv. Eine wesentliche Einschränkung erfährt die Anwendbarkeit durch die Begrenzung auf die Katalogstraftaten des § 100a Abs. 2 StPO. Betroffen sind deshalb nur Straftaten deren Höchststrafmaß mindestens fünf Jahre beträgt. Klassische, mithilfe von Computern oder dem Internet begangene Taten, z.B. Betrug, sind deshalb nicht eingeschlossen [GB09]. Eine Telekommunikationsüberwachung ist somit in der Regel nicht möglich.

2.2.3 Verwandte Untersuchungen

Im Rahmen unserer Literaturrecherche zur Erfassung der Thematik zeigte sich, dass die Diskussion stets in den Rechtswissenschaften stattfindet. Folgerichtig beschränkt sich diese bisher auf die juristischen Auswirkungen auf die Arbeit von Strafverfolgungs- und Ermittlungsbehörden – ohne Ansehen qualitativer bzw. quantitativer Aspekte oder gar der Behandlung des Phänomens auf Ebene der (Wirtschafts-) Informatik. Abb. 1 fasst deshalb die wesentlichen Arbeiten zusammenfassen.

Wesentliche Themen u. a.	**[3]**	**[4]**	**[12]**	**[13]**	**[21]**	**[22]**	**[23]**
(Un-) Zulässigkeit einer sog. Transborder Search	✓	✓	✓	✓	✓	✓	✓
Möglichkeiten eines (un-) mittelbaren Zugriffs beim Cloud Service-Provider	✓	✓	✓	✓	✓	✓	✓
Verwertbarkeit erlangter Beweismittel	✓				✓		✓

Abb. 1: Auswahl relevanter Untersuchungen

3 Methode

Ziel unserer Untersuchung war es herauszufinden, ob die geschilderte rechtliche Problematik tatsächlich zu Schwierigkeiten bei der Strafverfolgung führt. Eine Literaturanalyse führte zum Ergebnis, dass die Forschungsfrage bislang nicht beantwortet wurde. Aufgrund dessen haben wir eine qualitativ induktive, theoriengenerierende Vorgehens-

[3] In solchen Fällen kann ein förmliches Rechtshilfeverfahren angestoßen werden, welches allerdings äußerst zeitaufwändig und komplex ist. Grundsätzlich eröffnet die Cybercrime-Konvention (CCK) auch Handhabungsmöglichkeiten. Allerdings wurde diese nur von einer beschränkten Anzahl an Ländern ratifiziert und ist an strenge Regeln gebunden, die einer raschen Datensicherung entgegenstehen können.

weise gewählt [GL08] und insgesamt sieben qualitative Leitfadeninterviews durchgeführt. Die qualitative Inhaltsanalyse der Interviews folgte [Ma08]. Für die Durchführung der Gespräche wurde ein Leitfaden entwickelt. Die Erstellung erfolgte in Anbetracht der Thematik disziplinenübergreifend, so dass sowohl juristisches Knowhow als auch Kenntnisse der Wirtschaftsinformatik einflossen. Dieser interdisziplinäre Ansatz wurde auch für die konkrete Interviewsituation gewählt.

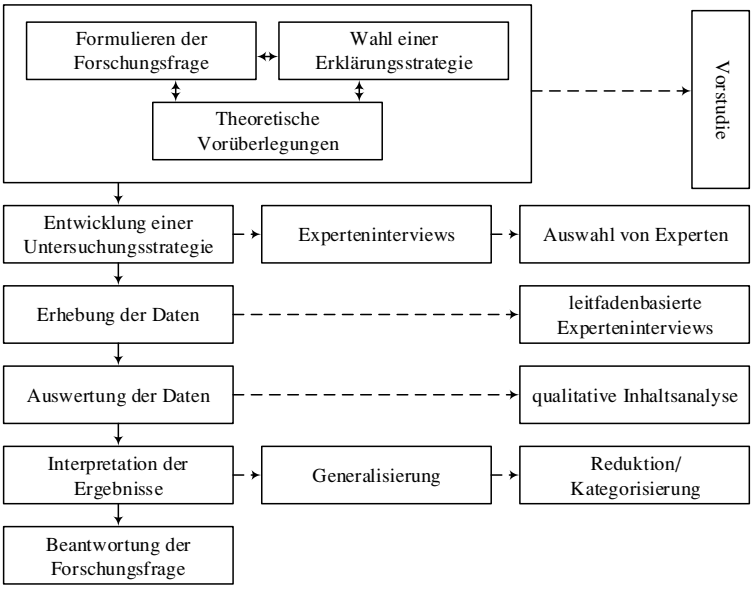

Abb. 2: Zugrundeliegender Prozess zur Beantwortung der Forschungsfrage

3.1 Erhebungsinstrument

Der Leitfaden zur Führung der Experteninterviews wurde aufbauend auf der geschilderten technischen Architektur eines Cloud Storage-Dienstes sowie der Ergebnisse der Literaturrecherche (vgl. Kapitel 2) entwickelt. Im Allgemeinen wird unter einem Experten eine Person verstanden, welche über ein spezifisches Rollenwissen verfügt, solches zugesprochen bekommt und diese besondere Kompetenz für sich in Anspruch nimmt [PW09]. Ziel bei der Auswahl der Interviewpartner war es dabei nicht, ein repräsentatives Abbild der gegenwärtigen Situation zu generieren. Vielmehr bestand dieses darin, Fachleute zu finden, die den Prozess von der Gesetzgebung, über die Strafverfolgung bis hin zur Forschung repräsentieren. Dabei handelt es sich um folgende Sample: (I) Politiker, (II) Staatsanwälte, (III) Richter, (IV) Wissenschaftler. Da die Justizverwaltung zum Kompetenzbereich der Bundesländer zählt, wurde zudem auf die Heterogenität der Dienstsitze geachtet.[4] Insgesamt konnten ein Bundespolitiker, drei Staatsanwälte, ein langjähriger Richter und Staatsanwalt sowie zwei Wissenschaftler gewonnen werden. Die Experten wurden zusätzlich danach ausgewählt, ob eine Befassung mit der zugrun-

[4] Auf eine Zuordnung der Bundesländer wird im Interesse des Daten- und Vertrauensschutzes verzichtet.

deliegenden Problematik als möglich erschien und sodann kontaktiert. Drei Interviews wurden aufgrund der zurückzulegenden Entfernung telefonisch geführt, während die Übrigen innerhalb eines persönlichen Termins stattfanden. Die Zusammensetzung der Interviewer war wiederum interdisziplinär (Rechtswissenschaftler und Wirtschaftsinformatiker). Ein Interview musste vorzeitig beendet werden,[5] nachdem der Interviewpartner nicht mehr bereit war, über die grundsätzliche Fragestellung hinaus zur Verfügung zu stehen. Als Abbruchkriterium wurden die Beantwortung unserer Forschungsfragen und das Ausbleiben neuerlicher Aspekte definiert; zumal die Feststellung des quantitativen Ausmaßes der Problematik – zunächst - nicht zielrelevant war [St04].

3.2 Auswertungsverfahren

Die Interviews wurden der qualitativen Inhaltsanalyse nach Mayring folgend ausgewertet. Dieses mehrstufige Verfahren, beinhaltet das Bilden eines Kategoriensystems als Kerninstrument [MA08]. Prinzipiell lassen sich auf Basis des sprachlichen Ausgangsmaterials, je nach Blickpunkt der Analyse, Aussagen in verschiedenen Richtungen treffen. So kann beispielsweise der im Text behandelte Gegenstand Ziel einer Inhaltsanalyse sein oder man könnte in einem anderen Fall etwas über die interviewte Person oder über die Wirkung des Textes auf eine bestimmte Zielgruppe herausfinden wollen [Ma08]. Die Forschungsfragen implizieren, dass der behandelte Gegenstand der Experteninterviews Thema der Inhaltsanalyse ist. Dies sind Aussagen der befragten Personen zum Thema Cloud Storage-Services vor dem Hintergrund strafprozessualer Gegebenheiten. Konkret wurde die Methode der Zusammenfassung gewählt [Ma08]. Ziel dieser Analysevariante ist es, das vorliegende Material zu reduzieren. Dabei sollen die wesentlichen Inhalte erhalten bleiben und mithilfe der Abstraktion ein überschaubarer Corpus geschaffen werden. Letzterer soll ein Abbild des vorliegenden Grundmaterials darstellen. Dabei werden durch verschiedene Instrumente, z.B. Generalisierungen und Bündelungen, abstrakte Aussagen gewonnen, die unter Kategorien subsumiert werden [LA95].

In einem ersten Schritt der zusammenfassenden, qualitativen Inhaltsanalyse werden zunächst die exakten Analyseeinheiten definiert: (a) *Kodiereinheit:* Jedwede Aussage des Befragten bezüglich Cloud Storage-Services im Kontext der Strafverfolgung, (b) *Kontexteinheit:* Fällt bei der gewählten Analysemethode mit der Kodiereinheit zusammen [Ma08], (c) *Auswertungseinheit:* Die Interviews werden chronologisch der Reihe nach ausgewertet.

Als Grundlage der Zusammenfassung wurde vorher das zugrunde gelegte Abstraktionsniveau definiert:

Es gilt möglichst allgemeingültige Aussagen im Hinblick auf Cloud Storage-Systeme sowie Aussagen über potentiell damit einhergehende Probleme im Kontext der alltäglichen Tätigkeiten von Strafverfolgungsbehörden zu extrahieren.

Exemplarisch für das verwendete Vorgehen wird in der Tabelle 1 eine Generalisierung mit anschließender Reduktion des Textes dargestellt.

[5] Im Folgenden: Interview 7.

Tab. 1: Beispiel für eine Aussagenreduktion

Zeile	Paraphrase	Generalisierung	Reduktion
493	Wir haben ja bei der Polizei diese regionalen Beweissicherungs- und Auswertungsstellen, die RBAs, vor Ort und da laufen auch entsprechende Schulungen. Also ich denke schon, dass man sich da der Problematik zunehmend bewusst wird.	Bewusstsein über die Problematik ist im Wesentlichen seitens der Staatsanwaltschaft und der Polizei vorhanden.	K2: Bewusstsein Cloud Storage

Nach Abschluss des Extrahierungsprozesses der Aussagen aus dem Ausgangsmaterial wurde das Kategoriensystem aufgestellt. Grundsätzlich bieten sich zwei Ansätze für die Kategorienbildung [Ma08]:

- Deduktive Kategorienbildung: Die Kategorien werden auf Basis der theoretischen Vorüberlegungen gebildet. Diese Kategorien werden im Vorfeld der Auswertung auf Grundlage des bisherigen Forschungsstandes oder neu entwickelter Theorien in einem Operationalisierungsprozess auf das zu analysierende Material hin entwickelt.
- Induktive Kategorienbildung: Die Kategorien werden unmittelbar aus dem Material extrahiert. Mittels eines Verallgemeinerungsprozesses werden diese unmittelbar während der Analyse gebildet - ohne sich auf vorab formulierte Theoriekonzepte zu stützen.

Vor dem Hintergrund der Forschungsfragen sowie der bisherigen Forschungen auf dem Gebiet erschien uns der induktive Prozess als fruchtbarer. Auf Grundlage der reduzierten Aussagen wurden in einem ersten Schritt „temporäre Kategorien“ gebildet. Anschließend wurden diese mithilfe von Bündelungen, Selektionen und Streichungen zu finalen Kategorien zusammengefasst.

4 Ergebnisse

Anhand des im vorstehenden Kapitel erläuterten methodischen Ansatzes konnten insgesamt neun Kategorien exzerpiert werden (Abb. 3). Nachfolgend werden diese Kategorien detailliert beschrieben.

Kategoriensystem	Int. 1	Int. 2	Int. 3	Int. 4	Int. 5	Int. 6	Int. 7
K1: Allgemeine Haltung	✓	✓	✓	✓	✓	✓	✓
K2: Bewusstsein Cloud Storage	✓	✓	✓	✓		✓	
K3: Datenauswertung		✓		✓	✓		
K4: Datenbereitstellung	✓			✓			
K5: Datenlokalisierung	✓	✓	✓	✓	✓	✓	
K6: Datenstandort	✓			✓		✓	
K7: Datenzugriff	✓			✓			
K8: Deliktarten	✓			✓			
K9: Erkennbarkeit	✓	✓					

Abb. 3: Ergebnisse der Experteninterviews

4.1 Kategorisierungen des Materials

K1: Allgemeine Haltung

Diese Kategorie bildet die Kernfrage unserer Arbeit ab; und zwar dahingehend, ob Cloud Storage-Angebote für Strafverfolgungsbehörden ein Problem darstellen. Diese Frage wurde von sämtlichen Interviewpartnern bejaht. Danach bestehen diese Schwierigkeiten im Wesentlichen darin, dass ein Strafverfolger wissen muss, wo die Daten lokalisiert sind und darin, dass sich die Daten im Ausland befinden können. Letzteres erfordert einen Zugriff via „Rechtshilfe oder anderen Überlegungen". Stellvertretend für diese Haltung steht die folgende Aussage: „Und da tritt eigentlich das Problem im Zusammenhang mit Cloud Computing auf, dass wir zwar auf die Daten zugreifen können […], aber wir haben das Problem, dass wir damit eigentlich wissen müssten wo die Daten lokal gespeichert sind, weil wir sonst in Probleme […] der Rechtshilfe oder anderen Überlegungen kommen."

K2: Bewusstsein Cloud Storage

Eingangs haben wir die Frage in den Raum gestellt, ob die mangelnde Diskussion des Themas in der Literatur darauf zurückzuführen sei, dass es bei den Bediensteten an einem Problembewusstsein mangelt. Dieses Thema wurde von fünf Interviewpartnern wahrgenommen. Inhaltlich muss dies hingegen differenziert werden. Während ein Experte die zunehmende Diskussion bei Konferenzen als Indiz für eine wachsende Sensibilität sieht, schränken dies drei Interviewpartner ein. Danach sei das Problembewusstsein nur „bei den jungen Kollegen relativ ausgebreitet, weil diese […] mit Cloud Computing […] groß werden." Ein Interviewter glaubt sogar, dass das „noch gar keiner so richtig gemerkt [hat]."

K3: Datenauswertung

Sofern Daten für die Verwertung in Ermittlungsverfahren vorliegen, handelt es sich oftmals um Massendaten. Gemäß den Aussagen unserer Experten stellt dies die ermittelnden Behörden oftmals vor Schwierigkeiten der Datenverarbeitung und Datenauswertung: „Das verursacht erhebliche Schwierigkeiten, weil sie natürlich einen immensen Auswertungsaufwand haben. Den Auswertungsaufwand versuchen sie ein stückweit zu kompensieren durch Auswertungsprogramme, die im polizeilichen Bereich eingesetzt werden. Nichtsdestotrotz ist es einfach dadurch extrem personal- und zeitaufwändig." Des Weiteren kann es dazu kommen, dass die vorliegenden Daten ausschließlich in verschlüsselter Form vorliegen und dementsprechend zunächst lesbar gemacht werden müssen: „Also Verschlüsselung ist ein Problem. Wir können Cloud Anbieter nicht zwingen den Schlüssel herzugeben. Was soll man machen, dann geht es halt nicht. Dann sind wir halt am Ende."

K4: Datenbereitstellung

Im Falle einer erfolgreichen Lokalisierung und eines erfolgreichen Zugriffs auf im Ausland gespeicherte Daten, stellt sich die Frage nach der Form der Datenbereitstellung. Diesbezüglich sind unterschiedliche Formen denkbar: „Also wenn ich Bestands- und Verkehrsdaten haben will, bekomme ich die in Form von Excel-Sheets oder Word-Dokumenten oder PDF-Dateien. Wenn ich Inhaltsdaten, will werden mir in aller Regel die entsprechenden Daten in Form von Festplatten oder DVDs zur Verfügung gestellt." Prinzipiell lässt sich jedoch festhalten, dass die übergebenen Datenträger zumeist forensisch auswertbare Kopien der zu sichernden Daten enthalten. Somit ist es möglich auch gelöschte Bereiche, beispielsweise einer Festplatte, auszuwerten und die gewonnenen Daten für ein entsprechendes Ermittlungsverfahren zu verwenden: „Das sind bitgetreue Kopien. Also wenn ich selbst einen Beschluss vollstrecke und bestimmte Daten spiegele, dann mache ich das in aller Regel in Form von bitgetreuen."

K5: Datenlokalisierung

Das Problem der Datenlokalisierung stellt ein Hauptproblem für Strafverfolgungsbehörden dar. Es wird in fünf Interviews dahingehend thematisiert, dass unklar ist, wo sich die Daten physisch befinden. Da für eine Standortlokalisierung – insbesondere während einer Durchsuchungsmaßnahme – keine (technischen) Hilfsmittel zur Verfügung stehen wird sich beholfen: „[…] Ich weiß der gilt nicht [Anmerkung: gemeint ist § 110 Abs. 3 StPO, der es gestattet, von einem Durchsuchungsobjekt auf einen Datenbestand außerhalb des Durchsuchungsobjektes zuzugreifen, sofern sich dieser innerhalb Deutschlands befindet], weil ich nicht weiß wo die Daten sind, aber mir bleibt ja gar nichts anderes übrig." Innerhalb der befragten Expertengruppe ist jedoch auch ein Fall vorzufinden, in welchem die Lokalisierung der Daten kein Problem darstellte und bereits im Vorfeld der Ermittlungen abgeklärt werden konnte: „Die Maßnahmen erstreckten sich auf vorab aufgeklärte Serverstandorte."

Festzustellen, in welchem Land sich die beweisbringenden Daten befinden, scheint - so lässt sich im Nachgang festhalten – die größte Herausforderung für Strafverfolgungsbehörden zu sein. Die Tatsache, dass die zu lokalisierenden Daten zum Teil fortwährend,

aufgrund der technischen Ausgestaltung von Cloud Storage-Services, ihren Standort wechseln, kommt erschwerend hinzu: „[…], darin begründet liegen, dass der physikalische Standort der Daten häufig nicht bekannt ist und auch wechselt."

K6: Datenstandort

Einem Interview lässt sich entnehmen, dass bereits erlebt werden musste, dass Daten nicht mehr lokal gespeichert werden: „Wir haben die Erfahrung in Ermittlungsverfahren gemacht, dass zunehmend eben Daten nicht mehr lokal gespeichert werden, sondern eben in vielen Verfahren, gerade im IT Bereich diese neuen Möglichkeiten technisch genutzt werden." Ein weiterer Befragter ist der Meinung, dass im Ausland gespeicherte Daten zu Problemen für die Strafverfolgung führen: „[…], das heißt wenn ich also positiv weiß, dass die Daten irgendwo anders liegen, wird es problematisch." Wohingegen ausgelagerte Daten innerhalb der Grenzen Deutschlands als unproblematisch gelten: „Wenn wir uns in Deutschland bewegen und die Daten auch hier sind, ist es rechtlich ohnehin kein Problem. Die Problematik tritt aus unserer Sicht immer erst ein, wenn wir Daten irgendwo in der ‚Cloud' ausgelagert haben."

K7: Datenzugriff

Sollte es dennoch gelingen die gesuchten Daten erfolgreich zu lokalisieren, so sieht man sich in der Praxis mit dem Problem des Datenzugriffs konfrontiert. Cloud Storage-Systeme können technisch so organisiert sein, dass unter Umständen der unmittelbare Datenzugriff aus Sicht der Strafverfolgungsbehörden gar nicht möglich ist: „[…]: „Ich kann ihnen die auch nicht rausnehmen, das ist ein RAID-System. Ich habe überhaupt keinen Zugriff."

K8: Deliktarten

Die Frage bei welchen Arten von Delikten die Problematik überhaupt auftritt, wird in zwei Interviews angesprochen: „Alles. Also dadurch, dass das Internet generell Tatmittel ist für alle denkbaren Straftaten, kann man das auch nicht begrenzen." Diese Meinung, dass prinzipiell bei jeder Straftat Beweismittel innerhalb eines Cloud Storage-Angebots zu finden sein können, deckt sich mit der Meinung eines weiteren Befragten: „Das kann man im Grundsatz gar nicht an bestimmten Deliktsgruppen festmachen. Das kann überall auftreten."

K9: Erkennbarkeit

Im Moment der Durchsicht eines Computers kann unter Umständen nicht ohne weiteres festgestellt werden, ob der Beschuldigte Cloud Storage-Dienste nutzt. Dieser Sachverhalt wird durch zwei Experten angesprochen. Denn die heutzutage übliche, kaum merkliche Einbindung derartiger Angebote in die Standard-Benutzeroberflächen eines Endgeräts führt zu Schwierigkeiten bei der Erkennbarkeit. Dies kann dazu führen, dass direkt während der stattfindenden Durchsicht Dateien gesichert werden, welche aus rechtlichen Gründen erst gar nicht hätten gesichert werden dürfen.

5 Zusammenfassung und Fazit

Obwohl wir uns bewusst sind, dass unsere Untersuchung nicht repräsentativ ist und die Durchführung von Interviews auch mit Verzerrungseffekten verbunden sein kann, möchten wir die zuvor präsentierten Ergebnisse festhalten:

- Cloud Storage-Dienste stellen deutsche Strafverfolgungsbehörden in der Praxis vor erhebliche operative technische und rechtliche Probleme.
- Diese Schwierigkeiten treten vor allem dadurch auf, dass die Daten zunächst lokalisiert werden müssen. Die Architektur der Services bedingt, dass zum Teil selbst den Anbietern der physische Datenstandort nicht bekannt ist. Hinzu kommt, dass sich der Datenstandort grundsätzlich ändern kann. Beide Punkte führen dazu, dass der Datenzugriff erschwert bzw. gar unmöglich sein kann. Langwierige Rechtshilfeersuchen können im Übrigen ins Leere führen, wenn sich der Datenstandort zwischenzeitlich geändert hat. Sollte beides tatsächlich gelungen sein, müssen die Dateien forensisch ausgewertet werden können. Dies scheint allerdings weniger problematisch zu sein, da die Provider – auch im eigenen Interesse[6] – entsprechende Kopien bereitstellen.
- Das Bewusstsein und die mangelnde Sensibilität für die Dienste, insbesondere für die technische und rechtliche Handhabe, scheinen nur bedingt vorhanden zu sein.

Alles dies zusammengenommen scheint die „Praxis“ mit einem pragmatischen - wenn auch rechtlich unsicherem – Vorgehen zu agieren: die relevanten Dokumente werden im Rahmen der Durchsuchungsmaßnahme beim Betroffenen/Beschuldigten (oder Zeugen) vor Ort gesichert – ohne der Frage nachzugehen, wo sich die Daten tatsächlich befinden. Ungeklärt ist bislang die Verwertbarkeit derart erlangter Beweismittel.

Daraus ergeben sich sowohl für die Wirtschaftsinformatik als auch für die Rechtswissenschaften Handlungsbedarf. Einerseits müssen die betroffenen Staatsanwälte und Richter, vor allem aber die Ermittlungsbeamte für die Thematik sensibilisiert werden. Andererseits müssen den Strafverfolgern technische Hilfsmittel – Tools oder Applikationen - zur Verfügung gestellt werden, die zum einen die Identifikation erlauben, ob der von einer Durchsuchung Betroffene Cloud Speicherdienste nutzt. Zum anderen müssen diese Hilfsmittel auch eine Lokalisierung des tatsächlichen Datenstandorts ermöglichen. Andererseits müssen die bilateralen oder supranationalen Normen, wie die Cybercrime-Konvention gelebt und weiterentwickelt werden.

Literaturverzeichnis

[AC11] Auer-Reinsdorff, A.; Conrad, I., Hrsg.: Beck’sches Mandats-Handbuch IT-Recht. C. H. Beck, München, 2011.

[BW10] Birk, D.; Wegener, C.: Über den Wolken: Cloud Computing im Überblick. In Datenschutz und Datensicherheit (DuD), 2010, 34; S. 641–645.

[6] Man denke an die Situation, dass eine Ermittlungsbehörde einen Server gänzlich vor Ort sicherstellen oder beschlagnahmen würde, um diesen zur Auswertung mitzunehmen.

[Bä11] Bär, W.: Transnationaler Zugriff auf Computerdaten. In ZIS, 2011, 6; S. 53–59.
[GB09] Gercke, M.; Brunst, P.W., Hrsg.: Praxishandbuch Internetstrafrecht. Kohlhammer, Stuttgart, 2009.
[GL08] Gläser, J.; Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse als In-strumente rekonstruierender Untersuchungen. VS Verlag für Sozialwissenschaften, Wiesbaden, 2008.
[Ge09a] Gercke, M.: Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden. In (Taeger, J.; Wiebe, A., Hrsg.): Inside the Cloud – Neue Herausforderungen für das Informationsrecht. Oldenburger Verlag für Wirtschaft, Informatik und Recht, Oldenburg, Göttingen, 2009; S. 499–507.
[Ge09b] Gercke, B.: Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten. Strafverteidiger Forum (StraFo), 2009; S. 271–274.
[Ge10] Gercke, M.: Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage. In CR, 2010; S. 345–348.
[Gi13] Girschner, S.: Storage-Markt in Deutschland: Starkes Datenwachstum fordert Unternehmen. In Digital Engineering Magazin, 2013.
[HW10] Heidrich, J.; Wegener, C.: Sichere Datenwolken – Cloud Computing und Daten-schutz. In MMR, 2010; S. 803–807.
[Ku11] Kudlich, H.: Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Prob-leme. Goltdammer's Archiv für Strafrecht (GA), 2011; S. 193–208.
[La95] Lamnek, S.: Qualitative Sozialforschung. Methoden und Techniken. Psychologie Verlags Union, Weinheim, 1995.
[Ma08] Mayring, P.: Qualitative Inhaltsanalyse. Grundlagen und Techniken. Beltz, Wein-heim, Basel, 2008.
[Ob10] Obenhaus, N.: Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft. In NJW, 2010; S. 651–655.
[PA09] Pohle, J.; Ammann, T.: Über den Wolken … – Chancen und Risiken des Cloud Computing. In Computer und Recht (CR), 2009; S. 273–278.
[PW09] Przyborski, A.; Wohlrab-Sahr, M.: Qualitative Sozialforschung – Ein Arbeitsbuch, 2009.
[RPZ10] Repschläger, T.; Pannicke, D.; Zarnekow, R.: Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale. In Praxis der Wirtschaftsinforma-tik (HMD), 2010, 47; S. 6–15.
[SR09] Schulz, C.; Rosenkranz, T.: Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen. In ITRB, 2009; S. 232–236.
[SUE13] Süptitz, T.; Utz, C.; Eymann, T.: State-of-the-Art: Ermittlungen in der Cloud. In Datenschutz und Datensicherheit (DuD), 2013, 37; S. 307–312.
[Sa08] Sankol, B.: Verletzung fremdstaatlicher Souveränität durch ermittlungsbehördliche Zugriffe auf E-Mail-Postfächer. In K&R, 2008; S. 279–284.
[Sc08] Schlegel, S.: „Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung. In HRRS, 2008, 9; S. 23–30.
[Si12] Sieber, U.: Straftaten und Strafverfolgung im Internet – Gutachten C zum 69. Deutschen Juristentag. C. H. Beck, München, 2012.