Der Elektronische Rechtsverkehr 40

Johanna M. Hofmann

Dynamische Zertifizierung

Datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung am Beispiel des Cloud Computing

Nomos

Der Elektronische Rechtsverkehr

Herausgegeben von
Prof. Dr. Alexander Roßnagel
in Zusammenarbeit mit
dem TeleTrusT Deutschland e.V.

Band 40

Johanna M. Hofmann

Dynamische Zertifizierung

Datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung am Beispiel des Cloud Computing

Nomos

Dissertation an der Universität Kassel
Fachbereich 07 Wirtschaftswissenschaften
Verfasserin Johanna M. Hofmann
Disputation am 27.2.2019

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Kassel, Univ., Diss., 2019

ISBN 978-3-8487-5917-0 (Print)
ISBN 978-3-8487-5917-0 (ePDF)

1. Auflage 2019

Vorwort des Herausgebers

Die Arbeit von Frau Hofmann befasst sich mit einem für Wirtschaft und Gesellschaft sowie das Verhältnis von Recht und Technik sehr aktuellen und bedeutsamen Thema, nämlich der Bewältigung datenschutzrechtlicher Probleme des Cloud Computing durch dynamische Zertifizierung. Cloud Computing ermöglicht, Speicherplatz, Rechenleistung und Software-Anwendungen nicht mehr selbst verfügbar halten zu müssen, sondern bedarfsabhängig aus dem Internet zu beziehen. Diese Ressourcen können von jedem internetfähigen Endgerät, jederzeit und an jedem Ort in Anspruch genommen werden. Diese Möglichkeiten reduzieren die Kapitalbindung und verbessern Arbeitsprozesse der Cloud-Nutzer. Cloud-Anbieter können durch dieses Bereitstellungsmodell ihre Kapazitäten besser ausnutzen. Sie bieten sie über das Modell des Cloud Computing anderen zur spontanen oder fest gebuchten Nutzung an. Cloud Computing verspricht daher große wirtschaftliche Vorteile und Entwicklungspotentiale für Anbieter und Nutzer.

Vielfach betrifft Cloud Computing personenbezogene Daten und unterfällt daher dem Datenschutzrecht. Dieses ordnet Cloud Computing überwiegend als Auftragsverarbeitung ein. Der Cloud-Nutzer ist der Auftraggeber und der Cloud-Anbieter der Auftragsverarbeiter. Diese Einordnung bewirkt nach Art. 28 und 29 DSGVO, dass die Datenverarbeitung zwar durch den Cloud-Anbieter durchgeführt wird, die datenschutzrechtliche Verantwortung aber beim Cloud-Nutzer verbleibt. Für den Cloud-Nutzer entstehen dadurch drei rechtliche Pflichten: Er muss einen geeigneten Auftragsverarbeiter, der die Einhaltung des Datenschutzrechts gewährleistet, auswählen, er muss die datenschutzgerechte Verarbeitung der von ihm gelieferten Daten kontrollieren und er muss ihn hinsichtlich der datenschutzgerechten Verarbeitung der personenbezogenen Daten anweisen. Diese Pflichten wörtlich zu erfüllen, ist für KMU gegenüber global anbietenden Internetkonzernen illusorisch.

Jedoch könnte eine datenschutzrechtliche Zertifizierung helfen, diese Pflichten zu erfüllen. Die Auswahl geeigneter Auftragnehmer kann Zertifizierung dadurch unterstützen, dass der Cloud-Nutzer sich einen durch ein datenschutzrechtliches Zertifikat als geeignet ausgewiesenen Cloud-Anbieter aussucht. Die Erteilung von Weisungen kann dadurch erfolgen, dass der Cloud-Nutzer einen zertifizierten, hinsichtlich seiner Datenschutzeigen-

schaften ausreichend beschriebenen Cloud-Dienst auswählt. Alternativ kann er durch Online-Befehle innerhalb eines solchen Dienstes datenschutzbezogene Alternativen wählen. Seiner Verantwortung für die Einhaltung des Datenschutzrechts kann er schließlich dadurch gerecht werden, dass er auf die Kontrolle durch den Zertifizierer und die Aufsichtsbehörde vertraut, die das Zertifikat widerrufen müssen, wenn wesentliche Voraussetzungen des Zertifikats nicht mehr vorliegen.

Diese Lösung des Problems datenschutzrechtlicher Verantwortung hat einen entscheidenden Nachteil: Er liegt in der Statik der Zertifizierung und in der beschränkten Effektivität der Kontrolle einerseits und in der dynamischen Entwicklung von Cloud Computing und Technikrecht andererseits. Das Zertifikat gilt in der Regel für drei Jahre, kann aber – genau genommen – die Konformität eines Cloud-Dienstes mit dem Datenschutzrecht nur für den Tag seiner Erteilung bestätigen. Nachfolgende Kontrollen des Cloud-Dienstes erfolgen allenfalls selten und dann nur in Form von Stichproben. Cloud Computing muss sich jedoch seiner Zielsetzung entsprechend ständig neuen Umständen anpassen. Und auch das Datenschutzrecht entwickelt sich in seiner Konkretisierung ständig weiter. Je älter ein Zertifikat ist, desto weniger kann es tatsächlich die Konformität des veränderten Cloud-Dienstes mit dem veränderten Datenschutzrecht bestätigen. Dieses Problem kann nur eine dynamische Zertifizierung, die – soweit dies automatisch prüfbar ist – die Konformität des Dienstes permanent oder wiederkehrend überprüft und bestätigt.

Eine Untersuchung, wie eine solche dynamische Zertifizierung von Cloud-Diensten gestaltet werden muss, um den beschriebenen Zielsetzungen gerecht zu werden und datenschutzrechtlichen Vorgaben zu entsprechen, bietet eine dreifache, gleichermaßen praktisch wie methodisch hochrelevante Herausforderung für eine interdisziplinär orientierte Rechtswissenschaft: Zum einen müssen in praktischer Hinsicht die datenschutzrechtlichen Vorgaben aus mehreren Rechtsbereichen geprüft werden, ob sie geeignet sind, die datenschutzrechtlichen Fragen, die eine dynamische Zertifizierung von Cloud Computing aufwirft, zu beantworten. Sofern dies nicht möglich ist oder an Grenzen stößt, ist zum anderen zu untersuchen, ob und wie diese durch den Rechtsanwender, den Gesetzgeber oder andere Regelsetzer fortentwickelt werden müssen. Schließlich ist zu klären, wie eine dynamische Zertifizierung von Cloud Computing technisch und organisatorisch gestaltet werden muss, um die rechtlichen Anforderungen an ein solches Verfahren zu erfüllen.

Hier setzt die Arbeit von Frau Hofmann an. Sie will die Frage beantworten, wie ein dynamisches Zertifizierungsverfahren am Beispiel des Cloud

Computing rechtsgemäß gestaltet werden kann. Mit der von ihr vorgelegten ersten monographischen Untersuchung der Rechtsfragen dynamischer datenschutzrechtlicher Zertifizierung von Cloud Computing füllt sie wesentliche Lücken im Recht modernster Informations- und Kommunikationstechniken. Indem sie sowohl die europa- und verfassungsrechtlichen Grundlagen für Cloud Computing und Zertifizierung als auch die wettbewerbs- und datenschutzrechtlichen Voraussetzungen, Ausgestaltungen und Ergebnisse von Zertifizierungsverfahren untersucht, bietet sie sowohl wertvolle Hinweise für das notwendige Rechtsverständnis gegenüber Zertifizierungsverfahren als auch grundlegende Hilfestellungen für die Praxis. Indem sie zeigt, wie die datenschutzrechtlich effektive rechtliche, technische und organisatorische Gestaltung von dynamischer Zertifizierung möglich sein könnte, trägt sie zur Bewältigung schwieriger grundlegender Fragen der rechtlichen Bewältigung technischer Dynamik bei.

Die Arbeit entstand zu großen Teilen im Rahmen der Mitarbeit von Frau Hofmann in dem Forschungsprojekt „Vertrauenswürdige Cloud-Services durch dynamische Zertifizierung qualitativer, datenschutzrechtlicher und sicherheitstechnischer Anforderungen: Next Generation Certification (NGCert)", das die Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel unter Leitung des Unterzeichners durchführte. Das Forschungsprojekt wurde vom Bundesministerium für Bildung und Forschung von 2015 bis 2017 unterstützt. Projektpartner waren das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) in München (Gesamtprojektleitung), das Fachgebiet Wirtschaftsinformatik der Technischen Universität München, das Fachgebiet Informationssysteme und Systemgestaltung der Universität Kassel, EuroCloud Deutschland und Fujitsu Deutschland. In diesem Forschungsprojekt bearbeitete Frau Hofmann selbstständig die hier untersuchten Rechtsfragen und konnte in enger interdisziplinärer Zusammenarbeit mit Informatikern, Betriebswirten und Praktikern interdisziplinären Fragen nachgehen.

Für die künftige Entwicklung und Gestaltung von dynamischen datenschutzrechtlichen Zertifizierungsverfahren sowie die rechtswissenschtliche Diskussion über diese ist zu hoffen, dass die Entscheidungsträger in Politik, Wirtschaft und Wissenschaft die Erkenntnisse dieser Arbeit zur Kenntnis nehmen und bei ihren Entscheidungen berüksichtigen.

Kassel, im März 2019 *Alexander Roßnagel*

Inhaltsverzeichnis

Tabellenverzeichnis

Danksagung

Die Arbeit wurde am 5. Juli 2018 fertiggestellt. Danach erschienene relevante Literatur und Rechtsprechung wurde vereinzelt bis zum 15. März 2019 nachgetragen.

Zahlreiche Personen haben durch vielfältige Unterstützung zum Gelingen dieser Arbeit beigetragen. Ihnen möchte ich an dieser Stelle meinen herzlichen Dank aussprechen.

Besonderer Dank gebührt meinem Doktorvater, Herrn Prof. Dr. Alexander Roßnagel – für das Forschungsthema, das mich sofort begeistert hat, und für die konstruktive Betreuung meiner Promotion. Dank ihm blicke ich auf knapp vier Jahre Forschung unter optimalen Bedingungen zurück, die man jedem Doktoranden nur wünschen kann. Dazu beigetragen haben natürlich auch meine Kollegen in der Projektgruppe verfassungsverträgliche Technikgestaltung, denen ich für die freundliche Arbeitsatmosphäre, wertvollen wissenschaftlichen Diskurs und umfangreiches Korrekturlesen danke. Herrn Prof. Dr. Wolfgang Thaenert danke ich für die wissenschaftliche Betreuung meiner Arbeit als Zweitgutachter.

Außerordentlicher Dank gebührt daneben einer ganzen Reihe von Menschen, die mich während der Zeit des Schreibens auf verschiedene Art und Weise unterstützt haben. Sie mögen mir nachsehen, dass ich ganz im Sinne des Datenschutzes auf eine namentliche Aufzählung verzichte.

Besonders hervorheben möchte ich aber dennoch zwei Menschen – Charlotte Husemann und Dominik Hoidn, die mir nicht nur freundschaftlich eng verbunden sind, sondern mich in ganz besonderem Maße auch fachlich während der Zeit des Schreibens begleitet und gemeinsam mit meinen Eltern die mühevolle Aufgabe des Korrekturlesens auf sich genommen haben. Ihnen beiden und meiner Familie, die mich stets unterstützt, widme ich diese Arbeit.

München, März 2019 *Johanna M. Hofmann*

Abkürzungsverzeichnis

a.F.	alte Fassung
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AkkStelleG	Akkreditierungsstellengesetz
Alt.	Alternative
ÄndBeschl.	Änderungsbeschluss
AnwBl	Anwaltsblatt (Zeitschrift)
Art.	Artikel
Az.	Aktenzeichen
BB	Betriebs-Berater (Zeitschrift)
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BDSG	Bundesdatenschutzgesetz
Bearb.	Bearbeiter/in
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMBF	Bundesministerium für Bildung und Forschung
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BRAO	Bundesrechtsanwaltsordnung
BR-Drs.	Bundesrats-Drucksache
BRJ	Bonner Rechtsjournal (Zeitschrift)
BSI	Bundesamt für Sicherheit in der Informationstechnik

bspw.	beispielsweise
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGG	Bundesverfassungsgerichtsgesetz
BVerwG	Bundesverwaltungsgericht
Berge	Entscheidungen des Bundesverwaltungsgerichts
BW	Baden-Württemberg
CR	Computer und Recht (Zeitschrift)
Cri	Computer Law Review International (Zeitschrift)
CRM	Customer-Relationship-Management
CuR	Computer und Recht (Zeitschrift)
DANA	Datenschutz Nachrichten (Zeitschrift)
ders.	derselbe
dies.	dieselbe
DIN	Deutsches Institut für Normung
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DSGVO	Datenschutz-Grundverordnung (EU) 2016/679 („Grundverordnung“)
DSGVO-E	Entwurf für eine Datenschutz-Grundverordnung
DSRL	Datenschutzrichtlinie (95/46/EG)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)
e.g.	exempli gratia (dt. zum Beispiel)
EG	Europäische Gemeinschaft
Eg.	Erwägungsgrund
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
et al.	et alii (und andere)
etc.	et cetera

EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGrZ	Europäische Grundrechte-Zeitschrift
EuR	Zeitschrift für Europarecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f.	folgende/-r/-s
ff.	fortfolgende/-r/-s
Fn.	Fußnote(n)
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GRCh	Charta der Grundrechte der Europäischen Union (Grundrechtecharta)
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
h.M.	herrschende Meinung
Hrsg.	Herausgeber/in
Hs.	Halbsatz
i.d.	in der/in dem
i.E.	im Ergebnis
i.S.d.	im Sinne des/der
i.S.e.	im Sinne einer/eines
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IaaS	Infrastructure as a Service
IP	Internetprotokoll
IPRB	IP-Rechts-Berater (Zeitschrift)
ISO	International Organization for Standardization
IT	Informationstechnik
ITRB	Der IT-Rechts-Berater (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	JuristenZeitung

K&R	Kommunikation & Recht (Zeitschrift)
Kap.	Kapitel
KMU	Kleine und mittlere Unternehmen
KOM	Dokument der EU-Kommission
LDSG	Landesdatenschutzgesetz
LG	Landgericht
LIBE	Ausschuss des Europäischen Parlaments für Bürgerliche Freiheiten, Justiz und Inneres
lit.	Litera (Buchstabe)
m.w.N.	mit weiteren Nachweisen
MMR	Multi-Media-Recht (Zeitschrift)
m.w.N.	mit weiteren Nachweisen
n.F.	neue Fassung
NIST	National Institute of Standards and Technology
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZBau	Neue Zeitschrift für Baurecht und Vergaberecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
o.g.	oben genannte/-r/-s
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
OLG	Oberlandesgericht
PaaS	Platform as a Service
PinG	Privacy in Germany (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RiStBV	Straf- und Bußgeldverfahren-Richtlinien
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
Rz.	Randziffer

SaaS	Software as a Service
SH	Schleswig-Holstein
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
SigV	Verordnung zur elektronischen Signatur (Signaturverordnung)
Slg.	Sammlung der Rechtsprechung des Gerichtshofes und des Gerichts Erster Instanz
sog.	sogenannte/-r/-s
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
TK	Telekommunikation(s-)
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.a.	unter anderem / und andere
UAbs.	Unterabsatz
u.U.	unter Umständen
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UN	United Nations (Vereinte Nationen)
UPR	Umwelt- und Planungsrecht (Zeitschrift)
USA	United States of America (Vereinigte Staaten von Amerika)
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom/von
verb. Rs.	verbundene Rechtssachen
VG	Verwaltungsgericht
VGH	Verfassungsgerichtshof
vgl.	vergleiche
VO	Verordnung
VuR	Verbraucher und Recht (Zeitschrift)
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz

WP	Working Paper
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZEV	Zeitschrift für Erbrecht und Vermögensnachfolge
ZEuP	Zeitschrift für Europäisches Privatrecht
zul. geänd. d.	Zuletzt geändert durch
ZUM	Zeitschrift für Urheber- und Medienrecht

1 Einleitung

Cloud Computing ist keine neue Technologie, sondern lediglich eine Nutzungsvariante herkömmlicher Technologien.[1] Es handelt sich dabei um ein „gesellschaftsweites Querschnittsthema",[2] ein „Paradigma",[3] das „nicht mehr wegzudenken" ist,[4] einen „Verkaufsschlager"[5], zentralen „Wachstumsmotor und Innovationstreiber mit dem Potenzial, die gesamte IT-Branche nachhaltig zu verändern".[6]

Tatsächlich nutzten im Jahr 2016 laut einer Studie der Wirtschaftsprüfungsgesellschaft KPMG AG in Zusammenarbeit mit der Bitkom Research GmbH 65 Prozent der befragten Unternehmen in Deutschland Cloud Computing-Dienstleistungen (Cloud-Dienste).[7] Darin liegt ein Anstieg von 25 Prozent im Vergleich zum Jahr 2014. Weitere 18 Prozent planten oder diskutierten im Jahr 2016 den Einsatz von Cloud Computing für die Zukunft. Im Zuge der fortschreitenden umfassenden Digitalisierung des Alltags wird der Bedarf an Cloud Computing-Angeboten weiterhin massiv

---

1 *Lenzer*, in: Conrad/Grützmacher 2014, 116; es ist insoweit von einer „Vertriebsart" (*Sujecki*, K&R 2012, 317), einem „Geschäftsmodell" (*Lehmann/Giedke,* CR 2013, 608; *Suchomski*, ITRB 2016, 90), einer „schnell wachsende(n) Methode" (*Sujecki*, K&R 2012, 312), weiterentwickeltem Outsourcing (*Schuster/Reichl*, CR 2010, 40), „Outsourcing 2.0" (*Seffer*, in: Conrad/Grützmacher 2014, 128), einer „populären Unternehmensstrategie" (*Roßnagel/Heinson/Bedner*, Wissensmagazin der TU Darmstadt 2010, 53), „einem der größten ökonomischen Trends" (*Pötters*, NZA 2013, 1055) oder gar einem „Verkaufsschlager" (*Schulz*, MMR 2010, 75) zu lesen.

2 *Roßnagel*, in: ders. 2015, 237.

3 BSI, C5, 2016, 5.

4 *Rath/Rothe*, K&R 2013, 623.

5 *Schulz*, in: Roßnagel 2015, 99.

6 *Schneider/Sunyaev* 2015, 1. Daneben wird Cloud als „perfect high tech storm" bezeichnet (*Mathews Hunt*, CLSR 2015, 451).

7 Im Rahmen des sogenannten „Cloud-Monitor 2017" wurden Ende 2016 stichprobenartig 554 Personen in Führungspositionen aus deutschen Unternehmen mit mindestens 20 bis über 2000 Mitarbeitern befragt. Der Cloud-Monitor 2017 ist auf dem Internetauftritt von KPMG unter kpmg.de abrufbar. Eine Trendanalyse von Netskope, die auf aggregierten und anonymisierten Daten von „Millionen von Nutzern" basiert, hat ergeben, dass Unternehmen im zweiten Quartal 2017 durchschnittlich 1022 Cloud-Dienste nutzen (abrufbar unter resources.netskope.com/h/i/366940901-september-2017-netskope-cloud-report, zuletzt abgerufen am 15.3.2019).

ansteigen.[8] Ein Unternehmen kann sich, will es wettbewerbsfähig bleiben, dem vielfach vorteilhaften Cloud Computing praktisch nicht mehr verschließen.[9] Denn selbst wenn Cloud Computing zunächst eine Frage des Prestiges gewesen sein mag, so wird es immer mehr zur Existenzfrage.[10]

1.1 Das Problem

Mit dem Zuwachs an Datenströmen steigen allerdings auch die Gefahren für die Grundrechte der Beteiligten und grundlegende gesellschaftliche Werte.[11] Schuld daran sind Wesensunterschiede zwischen Technik und Recht, die beim Cloud Computing besonders auffällig sind.

Gemeinsam ist Technik und Recht zwar, dass ihnen beiden großer Einfluss auf die Entwicklung des Einzelnen[12] und der Gesellschaft

---

8 Laut einer Studie werden bis in das Jahr 2020 im Unternehmensbereich allein in Deutschland im Vergleich zum Jahr 2015 Umsatzsteigerungen von knapp 260 Prozent prognostiziert (vgl. manage it, Umsatz mit Cloud Computing im B2B-Bereich in Deutschland von 2011 bis 2015 und Prognose für 2020 (in Milliarden Euro), in: Statista – Das Statistik-Portal, Zugriff am 8.11.2017, de.statista.com/statistik/daten/studie/165388/umfrage/prognose-zum-umsatz-mit-cloud-computing/. Vgl. auch *Roßnagel* 2017, 52; das hat auch die Europäische Kommission (fortan „EU-Kommission" oder schlicht „Kommission") erkannt und deshalb in der Europäischen Cloud-Initiative einen Plan für den Aufbau einer Cloud- und Dateninfrastruktur der Spitzenklasse für Wissenschaft und Technik dargelegt (s. Kommission, Cloud-Initiative 2016, passim). Die Cloud-Initiative ist Teil der Strategie für den Digitalen Binnenmarkt, einer der „Prioritäten" der Kommission (Kommission, Binnenmarktstrategie 2015, 3) und baut u.a. auf den Ergebnissen der Europäischen Cloud-Strategie (s. Kommission, Cloud-Strategie 2012) auf (Kommission, Cloud-Initiative 2016, 3).

9 So auch *Kremer*, in: Schwartmann u.a. 2018, Art. 28 Rn. 1; zu den Vorteilen s. 2.1.

10 *Roßnagel/Pfitzmann/Garstka* 2001, 21.

11 Das gilt erst recht für die empfundene Bedrohungslage. Vor dem Hintergrund von Erpressungstrojanern wie bspw. WannaCry stiegt die von Unternehmen empfundene Bedrohungslage laut einer Umfrage der Kompetenzgruppe Sicherheit im eco-Verband der Internetwirtschaft e. V. erheblich an. Von den 590 befragten Security-Experten gaben 95 % an, dass sie eine wachsende oder stark wachsende Bedrohungslage wahrnähmen. Eher skeptisch (57 %) äußerten sich die Befragten zu den Auswirkungen von Cloud-Diensten auf die IT-Sicherheit (s. eco Studie IT-Sicherheit 2017, abrufbar unter eco.de/wp-content/blogs.dir/eco_report_it-sicherheit-2017.pdf, zuletzt abgerufen am 15.3.2019).

12 Im Rahmen dieser Untersuchung wird anstelle einer Doppelbezeichnung der besseren Lesbarkeit halber für Personen- und Funktionsbezeichnungen die männliche Form gewählt, ohne dabei die weibliche Form auszuschließen.

zukommt.[13] Auch sind beide nicht erst seit der Erfindung des Computers eng miteinander verbunden[14] und aufeinander angewiesen. So muss Technik auf der einen Seite rechtlichen Vorgaben entsprechen, damit man sie überhaupt benutzen darf; auf der anderen Seite bedarf aber auch Recht zu seiner Durchsetzung in vielerlei Hinsicht moderner Technik. Darin offenbart sich zugleich der erhebliche Einfluss, den Technik auf Recht ausübt, wenn beispielsweise durch Innovation in der Kryptographie Sicherheitsmaßnahmen für einen Datenverarbeiter ohne erheblichen Aufwand erhältlich werden und damit rechtlich gefordert werden können.

Größer noch sind indes die mittelbaren Auswirkungen der Technik auf das Recht, das Konflikte im sozialen Zusammenleben regeln will und sich deshalb auch an faktische, durch Technik verursachte Veränderungen anpasst.[15] Grundlegende Unterschiede zwischen Technik und Recht führen gleichzeitig jedoch zu Vermittlungsproblemen, die einen genaueren Blick lohnen.

1.1.1 Vermittlungsprobleme zwischen Technik und Recht

Vermittlungsprobleme zwischen Technik und Recht zeigen sich erstens darin, dass innovationsfreudige Technik, die sich „explosiv“[16] fortentwickelt, einer schwerfälligen und äußerst langsamen Rechtsfortbildung gegenübersteht. Das Recht ist folglich bereits auf nationaler Ebene mit der technischen Innovationskraft „überfordert“.[17] Gänzlich unvereinbar mit der Geschwindigkeit und der Radikalität der Veränderungen der Informations-

13 *Roßnagel* 1993, 11ff. sowie 105ff.; *Hornung* 2005, 87.

14 Bereits 1980 trugen *Louis Brandeis* und *Samuel Warren* unter dem Titel „The Right to Privacy“ wesentlich zur Erkenntnis über Privatssphärenschutz bei, indem sie darin das berühmte „right to be let alone“ begründeten (*Warren/Brandeis*, HLR 1890, 193ff.). Dem Artikel waren zwei revolutionäre technische Innovationen vorausgegangen: Die Marktreife der Handkamera mit Rollenfilm und die Entwicklung moderner Tagespresse (s. ausführlich *Bendrath*, in: Sokol, 2008, 97f.).

15 *Roßnagel*, Der Staat 1983, 551ff.; wegen dieses Zusammenhangs wird zuweilen kritisiert, es sei in Mode, die „normative Kraft des Faktischen zu fürchten oder zu besingen und darüber die normative Kraft des Normativen zu vergessen“ (*Zeh*, in: Schirrmacher 2015, 36).

16 *Hassemer*, in: Liber Amicorum Simitis 2000, 129.

17 *Roßnagel*, in: Liber Amicorum Winand 2008, 383.

technik ist die gesetzgeberische Taktung auf Ebene der Europäischen Union (EU)[18] auf dem Gebiet des Datenschutzes.[19]

Zweitens verlangt das Recht aus Gründen der Flexibilität nach Abstraktheit,[20] um möglichst viele Sachverhalte erfassen zu können. Diese Abstraktion, wie sie insbesondere im Datenschutzrecht auftaucht, wirkt zuweilen als „realitätsfremde Fiktion".[21] Der Technikentwickler hingegen benötigt konkrete Vorgaben, eindeutig formuliert und mathematisch darstellbar. Hinzu kommen diverse weitere Wesensunterschiede, die eine Vermittlung zwischen Technik und Recht erschweren, wie beispielsweise die geographische Begrenztheit des Rechts, das dem Territorialprinzip unterliegt,[22] die der „körperlosen" Information[23] und technischen Möglichkeiten auf einem globalisierten Markt gegenübersteht, die auf Entgrenzung drängen.[24]

Drittens herrschen auf dem Gebiet des Technik- und Datenschutzrechts Regelungsdefizite, die sich insbesondere beim Cloud Computing zeigen. So ist etwa zu lesen, das deutsche Datenschutzrecht befinde sich wie kaum ein anderes Rechtsgebiet in einem „Nirwana zwischen gesellschaftlicher Bedeutung und fast vollständig fehlender Rechtssicherheit".[25] Zuweilen wird sogar bezweifelt, dass Datenschutzrecht überhaupt in der Lage sei, Vertrauen zu vermitteln.[26] Die Bedeutung von Vertrauen auf einem globalisierten Markt steigt mit der Anzahl der Akteure, die bei der Bereitstellung von Cloud-Diensten mitwirken.[27] Vertrauen ist entscheidend für jeden wirtschaftlichen Erfolg. Nachvollziehbare datenschutzfördernde

---

18 Soweit im Rahmen dieser Untersuchung von „Union" die Rede sein wird, ist damit die Europäische Union gemeint.

19 *Roßnagel*, DuD 2012, 553. Einer der Gründe liegt darin, dass Rechtsordnungen von kultureller Identität geprägt sind (*Rieß*, DuD 2002, 534).

20 *Simitis*, NJW 1998, 2479.

21 *Fetzer*, in: Sokol 2008, 57.

22 Begrenzend wirken die nationalstaatliche Souveränität und die erforderliche demokratische Legitimation (*Rieß*, in: Freundesgabe Büllesbach 2002, 253).

23 *Roßnagel*, in: Liber Amicorum Winand 2008, 383; vgl. zur „Globalität" des Internet *Roßnagel*, in: Kubicek 2002, 269f.

24 Vgl. *Rieß*, in: Freundesgabe Büllesbach 2002, 253; *Rieß,* DuD 2002, 533; s. für eine Analyse der Auswirkungen der Globalisierung auf den Datenschutz *Höffe*, in: Freundesgabe Büllesbach 2002, 257ff.

25 *Engeler*, Die Auftragsdatenverarbeitung braucht ein Reboot – mit der DSGVO in der Hauptrolle, in: www.telemedicus.info vom 24.11.2016.

26 Vgl. *Petersen* 2000, 120; a.A. *Roßnagel/Pfitzmann/Garstka* 2001, 21.

27 Zum Vertrauensverlust als „Sales Blocker" des Cloud Computing s. *Heckmann*, in: FS Würtenberger 2013, 35ff.

Maßnahmen wiederum sind wesentlich für das Vertrauen der Kunden.[28] Zwar hat die Datenschutz-Grundverordnung[29] in manchen Teilaspekten zu einem „Mehr" an Rechtssicherheit geführt,[30] bedauerlicherweise lässt sie jedoch jegliche Risikoadäquanz vermissen. Die Grundverordnung versteht sich selbst als technologieneutral,[31] verfolgt tatsächlich aber ein „überzogenes Verständnis" des Begriffs.[32] Technologieneutralität erscheint zwar insoweit sinnvoll, als Recht Innovationen nicht einschränken soll.[33] Insbesondere droht das in schnelllebigen Technikbereichen, in denen eine schwerfällige und langwierige Rechtssetzung entwicklungshemmend wirken würde. Allerdings ist die Grundverordnung nicht nur technik-, sondern gleichzeitig *risiko*neutral, da sie unabhängig von der Größe des Datenverarbeiters sowie dem Zweck und der Form der Datenverarbeitung dieselben Regeln für deren Zulässigkeit und die Rechte der betroffenen Personen vorsieht.[34] So fehlen spezielle Regelungen für Cloud Computing ebenso wie über allgemeine Rahmenbedingungen hinausgehende Vorgaben zur Zertifizierung. Ersteres ist besonders vor dem Hintergrund problematisch, dass die allgemeinen Regeln der Grundverordnung den spezifischen Grundrechtsrisiken, die Cloud Computing mit sich bringen kann, nicht gerecht werden.[35]

---

28 Vgl. *Roßnagel*, in: Freundesgabe Büllesbach 2002, 131.

29 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. EU 2016, L 119, 1, zul. Berichtigt duch Abl. EU 2018, L 127, 2, fortan „Grundverordnung" und „DSGVO" abgekürzt.

30 Zu nennen ist bspw. das umfangreiche Aufsichtsregime, das es Unternehmen künftig einfacher machen dürfte, die eine für sie zuständige Aufsichtsbehörde ausfindig zu machen (s. ausführlich *Hofmann*, in: Roßnagel 2018, § 6 Rn. 1ff.; zu den Befugnissen s. *Braun*, in: Roßnagel 2018, § 6 Rn. 47ff., sowie zur Kohärenz *Roßnagel*, in: ders. 2018, § 6 Rn. 85ff.).

31 Vgl. Eg. 15 DSGVO; *Reding*, ZD 2012, 198.

32 *Roßnagel/Geminn/Jandt/Richter* 2016, XVII.

33 So auch *Reding*, ZD 2012, 198; zum rechtswissenschaftlichen Innovationsbegriff s. *Hauschildt*, in: Hoffmann-Riem 1998, 29ff. Recht ist damit „Vorbedingung und Wegbereiter für technische Innovationen" (*Roßnagel*, in: Sauer/Lang 1999, 197).

34 *Roßnagel/Geminn/Jandt/Richter* 2016, XVII; *Roßnagel*, in: ders. 2018, § 1 Rn. 42.

35 So auch *Roßnagel*, in: ders. 2017, § 1 Rn. 42; zu den Risiken von Big Data und Profiling s. *Dammann*, ZD 2016, 313f.; das war im herkömmlichen Recht nicht anders, weshalb z.T. eine teleologische Auslegung der Pflichten der Auftragsdatenverarbeitung gefordert wurde (s. *Heckmann*, in: FS Würtenberger 2013, 17f. und 23ff.).

Problematisch ist viertens, dass der Datenschutz unter einem gewaltigen Vollzugsdefizit leidet,[36] das bei Internetdiensten besonders eklatant ist.[37] Schon früh wurde vor einer „Ohnmacht" des Staates gewarnt, die in eine Ohnmacht des Rechts münde, wenn dem Bürger keine ausreichenden Selbstschutzinstrumente zur Verfügung gestellt würden.[38] Und so verwundert es nicht, dass manch einer staatliche Aufsicht auf diesem Gebiet gar für eine „Wunschvorstellung" hält.[39]

1.1.2 Mehrdimensionale Intransparenz

Hinzu kommt eine mehrdimensionale Intransparenz, die besonders beim Cloud Computing zu Tage tritt und mit der Fortentwicklung der Technik und des Rechts sowie der fortschreitenden Globalisierung weiter zunimmt.[40]

Da ist erstens das Datenschutzrecht, das der Einzelne ohne vertiefte Fachkenntnis kaum mehr überschauen kann.[41] Beginnend mit der Frage, wo die Daten gespeichert sind[42] und nach welchem Recht der konkrete

---

36 *Walz*, in: Liber Amicorum Simitis 2000, 456; *Bäumler*, RDV 2001, 168; *Weichert*, RDV 2005, 1; *von Lewinski*, PinG 2013, 12ff.; *Roßnagel/Geminn/Jandt/Richter* 2016, XIX; von „Durchsetzungsdefizit" spricht *Bergt*, in: Kühling/Buchner 2018, Art. 42 Rn. 1; *Lachaud*, CLSR 2016, 818.

37 *Roßnagel/Richter/Nebel*, ZD 2013, 106; dies hat auch die EU-Kommission im Zusammenhang mit dem Verbraucherschutz erkannt (Kommission, Binnenmarktstrategie 2015, 5).

38 *Roßnagel*, in: Müller/Pfitzmann 1997, 377; *ders.*, ZRP 1997, 27.

39 *Lanier*, in: Schirrmacher 2015, 160.

40 Informationsasymmetrien herrschen nicht nur im Cloud-Bereich. Vielmehr ist in Zeiten steigender Unsicherheit hinsichtlich der Wahrheit verteilter Information auch die allgemeine Meinungsbildung vor neue Herausforderungen gestellt, wodurch das Bedürfnis für Verifikation merklich steigt.

41 So bereits *Podlech*, DVR 1976, 23; *Roßnagel/Pfitzmann/Garstka* bezeichneten im Jahr 2001 das Datenschutzrecht als „überreguliert, zersplittert", „unübersichtlich", „überkompliziert" und sogar „widersprüchlich" und gingen von über 1.000 Bundes- und Landesgesetzen und -verordnungen aus, die Datenschutzregelungen enthalten (vgl. *dies.* 2001, 29ff.); *Heckmann*, K&R 2010, 6; künftig wird das Nebeneinander von Unions- und nationalem Recht die Situation noch verkomplizieren. Der Überarbeitungsprozess des nationalen Rechts, das an die DSGVO angepasst werden muss, erfolgt in mehreren Stufen und wird nicht rechtzeitig bis zur Geltung der Grundverordnung am 25.5.2018 abgeschlossen sein. Entgegen ursprünglicher Hoffnung wird dies zu einer „hochkomplizierten Ko-Regulierung" führen (*Roßnagel*, in: ders. 2018, Vorwort).

42 *De Hert/Papakonstantinou/Kamara*, CLSR 2016, 21.

Sachverhalt zu beurteilen ist, erschwert die Komplexität der Rechtsordnungen das Auffinden der konkret daraus einschlägigen Normen, da selbst für Fachleute die Normenflut zuweilen unübersichtlich oder gar unverständlich ist.[43] Es drohen dadurch Einbußen an Effektivität.[44] Kompliziert ist aber auch die Anwendung und Auslegung der einschlägigen Regeln. Letztendlich drohen dem Rechtsunkundigen Abhängigkeit, Verunsicherung und Vereinsamung.[45]

Eine Besserung ist nicht in Sicht. So ist – im Gegenteil – mit Verabschiedung der Europäischen Datenschutz-Grundverordnung die Rechtslage noch weitaus komplizierter geworden. Ein Blick auf die mannigfaltigen Regelungsspielräume der Mitgliedstaaten zeigt, dass die allseits gepriesene Harmonisierung schnell an ihre Grenzen stößt. Eine Kollisionsnorm hält die Grundverordnung nämlich nicht vor, so dass künftig unklar sein wird, welches mitgliedstaatliche Recht auf eine Frage anwendbar ist, die in den einzelnen Mitgliedstaaten zulässigerweise unterschiedlich geregelt wurde. Das Fehlen einer internationalen Rechtsgrundlage wirkt sich auf dem Gebiet des Cloud Computing als besonderes Investitionshindernis aus. Die fortschreitende Globalisierung trägt dazu bei, dass sich diese Probleme weiter verstärken werden.

Zweitens ist auch die Her- und Zusammenstellung der Technik, das heißt der Aufbau der Dienste und die Zusammenstellung der Ressourcen in der Regel selbst intransparent.[46] Je höher die Komplexität beim Cloud Computing und je einfacher seine Bedienung, desto vorteilhafter ist es einerseits für den Nutzer.[47] Dadurch entsteht andererseits aber auch wieder ein Dilemma: Innovation, die eigentlich vereinfachen soll, birgt in Ermangelung entsprechender IT-Kompetenz der Nutzer[48] die Gefahr ihres endgültigen Kontrollverlustes. Im Ergebnis können nur „manisch-obsessive Technikfreaks (…) den Überblick" über die Datenschutzeinstellungen der

43 *Petersen* 2000, 114; *Fetzer*, in: Sokol 2008, 56; so im Zusammenhang mit dem Verbraucherschutz- und dem Vertragsrecht auch die Kommission, Binnenmarktstrategie 2015, 4.

44 *Roßnagel/Pfitzmann/Garstka* 2001, 32.

45 *Petersen* 2000, 84.

46 So zu technischen Produkten bereits im Jahr 1986 *Schmidt*, CuR, 1986, 259; *Roßnagel/Pfitzmann /Garstka* 2001, 28f.; *de Hert/Papakonstantinou/Kamara*, CLSR 2016, 17; Von „fast verschwindender Transparenz der IT-Systemlandschaft" ist sogar die Rede (*Kirn/Müller-Hengstenberg*, NJW 2017, 438).

47 *Lenzer*, in: Conrad/Grützmacher 2014, § 9 Rn. 53.

48 *Heckmann* sieht darin den Kern der Vertrauensbedürftigkeit (*ders*., K&R 2010, 7).

Anbieter behalten.[49] Mit sich akzelerierend fortentwickelnder Technik drohen sich Komplexität und Intransparenz künftig noch zu steigern.

Daraus folgt drittens, dass der Cloud Computing-Dienstleistungskunde (Cloud-Kunde)[50] und erst recht die betroffene Person,[51] deren personenbezogenve Daten vermittels Cloud-Diensten verarbeitet werden, möglicherweise gar nicht genau weiß, welche Cloud-Dienste er oder sie tatsächlich gerade nutzt[52] und wo seine oder ihre Daten aktuell gespeichert sind.[53] Denkbar ist auch, dass der Cloud Computing-Dienstanbieter (Cloud-Anbieter)[54] selbst auf Infrastruktur über einen Cloud-Dienst zurückgreift.[55] Ob diese Infrastruktur der eigenen Rechtsordnung unterliegt oder den eigenen Ansprüchen genügt, kann der Cloud-Kunde häufig nicht erkennen. Die Einbeziehung diverser weiterer Cloud-Anbieter und die Bildung von Auftragsketten ist bereits heute gängige Praxis. Auch prägt den Markt der Cloud-Angebote insgesamt hohe Intransparenz[56] und mangelnde Vergleichbarkeit sowohl der Anbieter als auch deren Angebote. Kaum miteinander vergleichbar sind unter anderem die von verschiedenen Anbietern unterstützten Sicherheitsmerkmale. Zudem mangelt es häufig an Standardisierung.[57] Absolute Transparenz ist vor diesem Hintergrund untypisch und auch kaum zielführend, da zu viel Information den Nutzer überfordern kann.[58] Es herrscht also häufig eine gewaltige Informationsasymmetrie zwischen den am Cloud Computing Beteiligten. Eine effektive Grundrechtsausübung setzt allerdings Kenntnis über die Tatsachen voraus. Mit anderen Worten erfordert informationelle Selbstbestimmung Information darüber, welche Gefahren bei der Verarbeitung personenbezogener Daten im Rahmen des Cloud Computing drohen.[59]

---

49 *Lanier*, in: Schirrmacher 2015, 160.
50 Zum Begriff der Cloud-Kunden siehe 2.2.
51 Zum Begriff der betroffenen Person siehe 2.2.
52 So auch Artikel 29-Datenschutzgruppe, WP 196, 7f.
53 Dieser Zustand wird als „nicht hinnehmbar" bezeichnet (s. *Söbbing*, in: Leible/Sosnitza 2011, 61).
54 Zum Begriff des Cloud-Anbieters siehe unten 2.2.
55 In diesem Beispiel böte der erstgenannte Cloud-Anbieter eine Anwendung, der zweitgenannte die Infrastruktur dazu an (vgl. dazu auch *Sunyaev/Schneider*, Commun. ACM 2013, 35).
56 *Stein/Schneider/Sunyaev*, HMD – Praxis der Wirtschaftsinformatik 2012, 33.
57 *Streitberger/Ruppel* 2009, 98.
58 *Kuhlen* 1999, 23.
59 So auch *Fetzer*, in: Sokol 2008, 61.

1.1.3 Mehrdimensionaler Kontrollverlust

Mit zunehmender Vernetzung und Virtualisierung geht schließlich selbst dann ein mehrdimensionaler Kontrollverlust einher, wenn eine betroffene Person selbst gar kein Cloud Computing nutzt, sondern ihre personenbezogenen Daten durch andere preisgegeben werden.[60] Digitale Enthaltsamkeit wird immer schwieriger. Künftig wird es immer weniger Menschen geben, deren personenbezogene Daten nicht im Internet verarbeitet werden.

Der Cloud-Kunde ist regelmäßig datenschutzrechtlich verantwortlich für die mittels des Dienstes verarbeiteten personenbezogenen Daten.[61] Ihn treffen Auswahl- und Überwachungspflichten gegenüber dem Cloud-Anbieter, denen er aufgrund der zunehmenden „Entörtlichung“[62] häufig tatsächlich nicht nachkommen kann. Die Folge sind Einbußen bei der tatsächlichen Beherrschbarkeit, die das Datenschutzrecht dem Cloud-Kunden aber abverlangt. Das gilt insbesondere, wenn der Cloud-Anbieter Rechenzentren im Ausland nutzt. Denn Virtualisierung und ortsungebundene Vernetzung gehören zu den wesentlichen Merkmalen des Cloud Computing. Selbst wenn der Cloud-Kunde den aktuellen Speicherort der personenbezogenen Daten kennt, für die er verantwortlich zeichnet, führen ad hoc zugewiesene Ressourcen zu kurzfristigen Veränderungen. Auch ist die regelmäßige persönliche vor-Ort-Kontrolle der Rechenzentren des Anbieters, der auf Ressourcen weiterer Cloud-Anbieter zurückgreift, häufig mit einem erheblichen Aufwand an Zeit und Kosten verbunden. Erschwerend kommt hinzu, dass aus Gründen der Redundanz zwischen den einzelnen Rechenzentren oft große Entfernungen liegen.[63] Kontrolleinbußen drohen daneben aber auch durch die Verwendung proprietärer technischer Lösungen und durch fehlende Interoperabilität und Standardisierung.[64]

Der Cloud-Anbieter muss zu Kontrollzwecken zwar grundsätzlich jedem seiner Kunden den Zutritt zu seinen Serverräumen gewähren. Der drohende „Prüftourismus“ würde jedoch risikoerhöhend wirken und ebenfalls zu einem Kontrollverlust führen. Die Alternative, die Auswahl der Cloud-

60 *Heymann,* CR 2015, 809; *Schaar/Onstein*, BRJ 2011, 126.
61 S. 3.3.3.1.3.
62 Zum Begriff s. *Schaar/Onstein*, BRJ 2011, 129.
63 *Niemann/Hennrich*, CR 2010, 691.
64 Kommission, Binnenmarktstrategie 2015, 16; Die Rede ist häufig von einem sog. Vendor Lock-in, soweit ein Cloud-Kunde mangels Standardisierung den Cloud-Anbieter nicht einfach wechseln kann.

Anbieter auf diejenigen zu beschränken, die örtlich erreichbar sind, widerspräche allerdings dem Wesen des Cloud Computing.[65]

Hinzu kommt häufig ein wirtschaftliches Machtungleichgewicht zwischen den Parteien eines Cloud-Vertrages, das daher rührt, dass der Cloud-Anbieter nicht selten ein wirtschaftlich starkes Unternehmen sein wird.[66] Dieses Ungleichgewicht erschwert es dem Cloud-Kunden, den gesetzlichen Anforderungen an Weisungs- und Kontrollrechte zu entsprechen.[67] Beim Geschäftsmodell des Cloud Computing ist die strikte Herrschaft des Cloud-Kunden über Verfahren und Daten also weder möglich noch erwünscht.[68]

Wenn bereits der Vertragspartner des Cloud-Anbieters Kontrollverlust beklagen wird, gilt das erst recht für die betroffene Person, deren personenbezogene Daten „in der Cloud" verarbeitet werden.[69] Die Fernwirkungen übermäßiger Datenpreisgabe für ihre Grundrechte bleiben häufig diffus.[70] Der Kontrollverlust wird dabei als größere Bedrohung wahrgenommen, als ein durch Cloud Computing möglicherweise ausgelöster Anstieg an Cyber-Kriminalität.[71] Beherrschbarkeit der eigenen personenbezogenen Daten ist aber notwendig, damit die betroffene Person ihre Rechte auf informationelle Selbstbestimmung und Datenschutz ausüben kann. Erforderlich ist dafür, dass Datensicherheit, Verfügbarkeit und Datenschutz[72] durch technische und organisatorische Maßnahmen im ausreichenden Umfang sichergestellt sind und der unberechtigte Zugriff durch Dritte auf die Daten ausgeschlossen ist.[73]

1.1.4 Mangelhafte Nachweisbarkeit

Es besteht neben dem genannten Kontrollverlust zudem die Gefahr, dass der Cloud-Kunde und die betroffene Person nicht oder zu spät Kenntnis von eventuellen Verstößen gegen datenschutzrechtliche Vorgaben erhalten und deshalb ihre Rechte, und im Falle des Cloud-Kunden auch Pflichten

65 *Selzer*, DuD 2013, 215 (216); s. dazu auch 2.
66 So auch *Hornung*, in: Auerhammer 2018, Art. 42 Rn. 77.
67 *Schaar/Onstein*, BRJ 2011, 129.
68 *Heckmann*, in: FS Würtenberger 2013, 21.
69 Artikel 29-Datenschutzgruppe, WP 196, 2,6f.
70 *Heckmann*, in: Hromadka u.a. 2009, 102f.
71 *Bigo et al*, Cybercrime-Studie 2012, 12.
72 Zum Unterschied zwischen Datenschutz und Datensicherheit s. 3.3.1.
73 *Bosesky/Hoffmann/Schulz*, DuD 2013, 95 (99).

gegenüber den betroffenen Personen, nicht oder nur beschränkt ausüben, beziehungsweise erfüllen können.

Mit der technischen Entwicklung verbreitet sich zum einen ein Bewusstsein für die Notwendigkeit eines starken Datenschutzes.[74] In Zeiten immer enger getakteter Hiobsbotschaften über Datenpannen,[75] gezielte Ausspähung und Überwachung[76] sowie weltweite Cyberattacken durch Schadsoftware[77] steigt zum anderen sowohl auf Verbraucher- als auch auf Unterneh-

---

74 Im Jahr 2015 hatten lediglich 15% der Europäer vollstes Vertrauen in Unternehmen wie Betreiber von Suchmaschinen, sozialen Netzen und E-Mail-Diensten, während 72% der Internetnutzer Bedenken hatten, dass zu viele ihrer personenbezogenen Daten online abgefragt würden (Kommission, Binnenmarktstrategie 2015, 15). Zudem gaben in der o.g. Studie der KPMG 73 Prozent der befragten Unternehmen an, dass sie Datenschutz in der Public Cloud für zumindest schwieriger halten, als in internen IT-Strukturen (Cloud-Monitor 2017).

75 So waren bei einer Datenpanne der Post im Jahr 2017 ca. 200.000 Umzugsmitteilungen der Post unverschlüsselt im Internet abrufbar, s. *Böck*, „Kundendaten: Datenleck bei der Deutschen Post", Zeit online vom 5. Juli 2017; s. *Sauerwein*, „200.000 Kundendaten der Post landen im Internet", wdr.de vom 05.7.2017; Handynummern und E-Mail-Adressen einer ungenannten Anzahl von Nutzern der Plattform Instagram wurden im dritten Quartal 2017 laut einer Mitteilung des Unternehmens durch einen Programmierfehler offengelegt; die Mitteilung ist abrufbar unter blog.instagram.com/post/164871973302/170901-news, zuletzt abgerufen am 15.3.2019; zudem stieg laut Bayerischem Landesamt für Datenschutzaufsicht die Anzahl der gemeldeten Datenpannen im Jahr 2016 im Vergleich zu den vorangegangenen Jahren überraschend an s. *Schulzki-Haddouti,* „Bayern: Gemeldete Datenpannen nehmen massiv zu", heiseonline.de vom 3. März 2017; s. eine chronologische Darstellung großer Datenpannen bis ins Jahr 2016 auf http://datenleck.net/.

76 Genannt seien hier bspw. die Enthüllungen *Edward Snowdens* der planmäßigen Überwachung durch die National Security Agency (NSA) von 2013, s. z.B. *Greenwald*, NSA collecting phone records of millions of Verizon customers daily, The Guardian v. 6. Juni 2013; oder aber die massenhafte, anlasslose Speicherung von Fluggastdaten, „Flugreisen: Datenschützer kritisieren lange Speicherung von Fluggastdaten", Spiegel online vom 9. November 2017, abzurufen unter spiegel.de/netzwelt/netzpolitik/fluggastdaten-speicherung-datenschuetzer-kritisieren-lange-speicherfristen-a-1177232.html, zuletzt abgerufen am 15.3.2019.

77 So z.B. der weltweite Angriff mit der Ransomware WannaCry im Mai 2017, die eine Microsoft-Sicherheitslücke genutzt und in Krankenhäusern, Telekommunikationsfirmen und weiteren Unternehmen Computerdaten verschlüsselt und Lösegeld gefordert hat, s. z.B. *Sagatz*, „Ransomware 'Wanna Cry' Wie Hacker mit Cyber-Attacken Millionen erpressen, Tagesspiegel vom 13. Mai 2017; *Beuth*, „Es ist zum Heulen – Hunderttausende Rechner sind von der Erpressungssoftware WannaCry befallen. Was die Opfer jetzt tun – und die Täter, Zeit online vom 15. Mai 2017.

mensseite das Bedürfnis nach Nachweisen über die Einhaltung datenschutzrechtlicher Anforderungen.

Damit er in einem potenziellen Verwaltungs- oder Gerichtsverfahren eine Vertrags- oder Grundrechtsverletzung nachweisen kann, muss der Antragssteller oder Kläger zudem verlässliche Nachweise erbringen. Angesichts des beschriebenen Kontrollverlusts und der mehrdimensionalen Intransparenz wird er solche Nachweise allerdings kaum erlangen können. Dies umschreibt ein Folgeproblem des Cloud Computing, dem nur durch Transparenz begegnet werden kann. Transparenz wiederum setzt erstens das Erfassen einer breiten Tatsachengrundlage voraus, die zweitens für betroffene Personen und Cloud-Kunden auch zugänglich ist.

1.1.5 Beschränkte Abhilfe durch herkömmliche Zertifizierungsverfahren

Die Kräfte des Wettbewerbs können zu einer Verbesserung des Datenschutzes und der Datensicherheit beitragen.[78] Datenschutz wurde frühzeitig als Wirtschaftsfaktor anerkannt.[79] Anstatt Datenschutz durch eine flächendeckende Verarbeitungsüberwachung oder durch Zwang durchzusetzen, sollten „eine funktionsfähige Kultur der Privatheit“[80] und ein lebendiger Datenschutz-Wettbewerb realisiert werden. Datenschutz sollte nicht *gegen*, sondern *mit* den datenverarbeitenden Stellen durchgesetzt werden.[81] Dahinter steht der Gedanke einer „civil information society“, in der die individuellen Nutzungsmöglichkeiten der Technik die Verwirklichungsbedingungen der Grundrechte nicht nur wahren, sondern sogar verbessern.[82]

Indem sie die Förderung von beispielsweise Selbstregulierungskonzepten[83] und kooperativen Ansätzen vorschreibt, nutzt die Datenschutz-

78 S. *Roßnagel,* in: Bäumler/v. Mutius 2002, 116.

79 Vgl. ausführlich *Büllesbach*, RDV 1997, 239ff. Ein Unternehmen, dessen Organisation geltendem Datenschutzrecht entspricht, gilt an sich als „deutlich“ werthaltiger, als eines, das diese Anforderungen nicht erfüllt (*Grützmacher*, CR 2017, 706).

80 *Weichert*, RDV 2005, 1.

81 *Krings/Mammen*, RDV 2015, 232.

82 *Roßnagel*, ZRP 1997, 30.

83 Selbstregulierung versteht die EU-Kommission als „Möglichkeit, dass Wirtschaftsteilnehmer, Sozialpartner, Nichtregierungsorganisationen oder Verbände untereinander und für sich gemeinsame Leitlinien auf europäischer Ebene (unter anderem Verhaltenskodizes oder sektorale Vereinbarungen) annehmen.“, EU-Kommission, Interinstitutionelle Vereinbarung „Besser Rechtssetzung“, Nr. 22.

Grundverordnung die Wirkung des Wettbewerbs für den Datenschutz.[84] Dadurch kann das Datenschutzrecht seinen Ruf als bürokratisches Hindernis ablegen und „neue Konturen als Wettbewerbsvorteil, als Beratungsgegenstand, als Dienstleistung, als Produktidee und als Aspekt der Selbstbestimmung“[85] gewinnen. Datenschutzrecht kann also sogar attraktiv werden.[86] Allerdings erfordert dies Rahmenbedingungen für Anreize, damit datenverarbeitende Stellen ein Eigeninteresse am datenschutzrechtgerechten Verhalten entwickeln[87] und demonstrieren.

Eine solche Maßnahme ist die datenschutz- und datensicherheitsrechtliche Zertifizierung. Die grundsätzliche Anerkennung von Zertifizierungsverfahren durch die Datenschutz-Grundverordnung ist auf dieser Ebene und mit dieser Reichweite ebenso einzigartig wie neu. Zertifizierungsverfahren führen dazu, dass Datenverarbeiter Datenschutz immer mehr als „Kundenbindungsinstrument“[88] wahrnehmen. Da sich die Grundverordnung auf Rahmenbedingungen für das Zertifizierungsverfahren beschränkt, muss dieses weiter ausgestaltet und geformt werden. Erforderlich ist ein System, das mit dem verfassungsrechtlichen Grundverständnis unserer Gesellschaft in Einklang ist und den gesellschaftlichen Ordnungszielen entspricht. Gleichzeitig muss ein solches System aber auch der Dynamik und Schnelllebigkeit des Gebiets des Prüfobjekts – Cloud Computing – gerecht werden und darf so der Innovation nicht im Wege stehen, sondern sollte diese fördern.[89] Dabei wird das Zertifikat zum stellvertretenden Bezugsobjekt des Vertrauens des Nutzers gemacht. Von diesem Vertrauensvorschuss und der vertrauensfördernden Wirkung eines Zertifikats profitieren letzten Endes der Cloud-Anbieter, der eigenständig nicht dazu in der Lage wäre, das erforderliche Vertrauen aufzubauen, und mittelbar auch der Cloud-Kunde.

---

84 S. zum Wettbewerb durch Datenschutz bereits *Roßnagel*, in: Freundesgabe Büllesbach 2002, 132.

85 *Roßnagel*, in: Bäumler/v. Mutius 2002, 124.

86 So bereits *Roßnagel/Pfitzmann/Garstka* 2001, 34.

87 S. *Roßnagel*, in: Freundesgabe Büllesbach 2002, 132; *Hornung/Hartl*, ZD 2014, 220.

88 Zum Begriff *Schaar*, DuD 2007, 259.

89 Innovation ist kein Rechtsbegriff, sondern eröffnet vielmehr Ordnungsaufgaben des Staates (*Roßnagel*, in: Hof/Wengenroth 2007, 9ff.), ihr kommen sowohl hemmende, aber auch lenkend-fördernde Wirkungen zu (*Roßnagel*, in: Hof/Wengenroth 2007, 13ff.).

Allerdings können Vielfalt und mangelnde Vergleichbarkeit des Angebots an Zertifizierungsverfahren[90] eine Bewertung und Interpretation erforderlich machen, die den Nutzer wiederum überfordern. Zudem verschleiern herkömmliche Zertifizierungsverfahren, die sich auf Momentaufnahmen beschränken, ohne auf die dynamische Entwicklung auf dem Gebiet des Cloud Computing einzugehen, den tatsächlichen Status Quo, da sie nicht in der Lage sind, auf Störungsfälle und Probleme zu reagieren. Von Veränderungen der tatsächlichen, rechtlichen oder technischen Gegebenheiten bleibt die Zertifikatsaussage unbeeindruckt. Ein herkömmliches Zertifikat suggeriert vielmehr einen Zustand, der möglicherweise so nicht mehr besteht und begründet damit tatsächlich unberechtigtes Vertrauen der Marktteilnehmer. Es ist noch nicht einmal sichergestellt, dass der Cloud-Anbieter im Fall von Sicherheitsvorfällen die Werbung mit dem Zertifikat einstellt. Allerdings muss auch nicht jedes Ereignis zertifikatsrelevant sein. Entscheidend ist schließlich auch, wie der Cloud-Anbieter mit einem Ereignis umgeht. Soll Cloud Computing erfolgreich sein, ist also eine Kultur konstruktiver Problemlösung erforderlich,[91] die alle Beteiligten einbezieht.

1.2 Die Lösung

Die Lösung des Problems liegt darin „Vertrauen in Technik durch Technik“[92] zu generieren und der festgestellten Dynamik mit Dynamik zu begegnen. Ein dynamisches Zertifizierungsverfahren vermag alle genannten Defizite herkömmlicher Verfahren[93] auszugleichen und gleichzeitig die aufgezählten Probleme bei der Annäherung von Recht und Technik zu überwinden, die auf dem Gebiet des Cloud Computing besonders eklatant in Erscheinung treten.[94]

Vereinfacht gesagt, bedeutet dynamische Zertifizierung kontinuierliche Überwachung von Verarbeitungsvorgängen im Rahmen eines Cloud-Dienstes und ereignisadäquate externe Evaluation des Gemessenen durch unabhängige Prüfer. Das Ergebnis ist eine stets aktuelle Zertifizierung, die

90 Ausführlich dazu *Feik/v. Lewinski*, ZD 2014, 59ff.; *Rüdiger* 2008, 160ff.
91 Heckmann, in: FS Würtenberger 2013, 39f.
92 Zum Begriff s. bereit *Müller/Pfitzmann*, in: dies. 1997, 11.
93 S. 1.1.5.
94 S. 1.1.

die tatsächlichen Gegebenheiten widerspiegelt und damit für echte Transparenz sorgt.

Es stellt sich jedoch die Frage, wie eine solche dynamische Zertifizierung technisch und normativ auszusehen hat. Grundsätzlich gilt: Zur Steuerung sozialer Veränderung muss technischer Fortschritt reflektiert gestaltet werden. Anstatt im Nachhinein die Folgen technischer Innovation zu regeln, ist es sinnvoller, wenn das Recht bereits auf die Gestaltung von Technik einwirkt.[95] Mit anderen Worten ist „den Konsequenzen der Technologie durch die Technologie selbst zu begegnen".[96] Die Gestaltung von rechtsverträglicher[97] Technik begegnet allerdings vielfältigen Problemen, die sich im Wesentlichen auf die Interdisziplinarität der Aufgabe und die verschiedenen Interessenslagen zurückführen lassen, die dabei zu berücksichtigen sind. Es ist Aufgabe interdisziplinärer Forschung, die verschiedenen Strebungen und Interessen zu untersuchen und in Einklang miteinander zu bringen, das heißt „Entwicklungskorridore aufzuzeigen, in denen sich die einzelnen Anstrengungen nicht konterkarieren".[98]

Die Schwierigkeit liegt darin, dass es die Öffnung gegenüber dynamischen Veränderungsprozessen erforderlich macht, „gleichsam eine Ex-post-Bewertung des Neuen zu antizipieren".[99] Es gilt dabei zudem, einen Wesensunterschied der beiden in Rede stehenden Disziplinen Recht und Technik zu beachten. Technik und Recht hängen – wie bereits festgestellt – voneinander ab und beeinflussen einander.[100] Insbesondere muss Recht „normativen Erwartungen, die sich in der Praxis bewährt haben, gegenüber Enttäuschungen sichern und gleichzeitig Veränderungen zulassen".[101] Recht ist an Sprache gebunden und existiert nicht in der Welt der realen Dinge. Nicht so dagegen die Technik.[102] Nach einem systemfunktionalen Verständnis zielt Technik anders als das Recht nicht auf Sinndeutung und

95 *Schaar/Onstein*, BRJ 2011, 131; *Hassemer*, in: Liber Amicorum Simitis 2000, 128; *Heckmann*, K&R 2010, 5; *Roßnagel* 1993, 16ff.; *Sydow 2017/Krings*, ZD 2014, 267.

96 *Simitis*, NJW 1998, 2478.

97 Rechtsverträglichkeit ist mehr als Rechtmäßigkeit, weil sie im Unterschied zu letzterer von einem veränderbaren normativen Maßstab ausgeht (*Roßnagel* 1993, 192ff.); „gemeinwohlrichtiges" Technologierecht fordert *Denninger* 1990, 35.

98 *Wegenroth*, in: Hof/Wengenroth 2007, 3.

99 *Wegenroth*, in: Hof/Wengenroth 2007, 4; so ähnlich bereits *Podlech*, DVR 1976, 23.

100 S. bereits *Breuer*, AöR 1976, 46ff.; zu den Wechselwirkungen von Technik und Recht s. *Jandt* 2008, 37ff.; *Vieweg*, Technik und Recht, in: Festgabe Lukes 2000, 201ff.; *Vieweg*, JuS 1993, 894 (895).

101 *Vesting*, in: Berg u.a. 2001, 23; *Kloepfer*, NuR 1997, 417f.

102 *Marburger*, in: Rüthers/Stern 1984, 277.

Geltung, sondern auf Gestaltung und Veränderung, indem sie die Herstellung und Nutzung „materieller, energetischer und informationeller Umwandlungs-, Speicherungs- und Transportsysteme“ umfasst.[103]

Wie das Cloud Computing selbst, bedarf die datenschutzrechtliche Zertifizierung folglich nicht nur der empirischen Akzeptanz, sondern auch der normativen Akzeptabilität.[104] Erforderlich sind strukturelle Lösungen in Form von lernfähigen Systemen, die auf sich verändernde Herausforderungen eingehen und entsprechend neue Antworten liefern können.[105] Diese innovativen Lösungen sollten möglichst auf die Bedürfnisse der einzelnen Marktteilnehmer individuell anpassbar sein. Damit sollen für Politik und Wirtschaft Spielräume zurückgewonnen werden, die Verteilungskämpfe zu entschärfen und inneren Frieden zu bewahren helfen.[106]

1.3 Gegenstand der Untersuchung und deren Grenzen

Diese Arbeit will aufzeigen, wie ein dynamisches Zertifizierungsverfahren am Beispiel des Cloud Computing rechtsgemäß gestaltet werden kann. Auf der Basis der Analyse des einschlägigen Rechts wird dazu zunächst das dynamische Zertifizierungsverfahren ausgestaltet und im Anschluss das Recht exemplarisch fortentwickelt.

Im Einzelnen wird sich diese Untersuchung der Wechselwirkung von Technik und Recht im Zusammenhang mit datenschutz- und datensicherheitsrechtlichen Zertifizierungsverfahren widmen, die Cloud-Dienste zum Gegenstand haben. Es wird ein Lösungsweg entwickelt werden, der die genannten Widersprüche möglichst auszuräumen, zumindest aber abzumildern in der Lage ist. Obgleich die detaillierte Regelung noch nicht existenter Technologien kaum möglich ist,[107] kann technikadäquate Normierung selbst dynamische Elemente beinhalten, um entwicklungsoffen technologischer Entwicklung längerfristig gerecht zu werden. Das zu entwickelnde dynamische Zertifizierungskonzept erfordert einerseits die rechtsverträgliche Gestaltung der Technik, andererseits eine technikadäquate Rechtsfortbildung. Beides wird diese Untersuchung behandeln. Da es eine dynamische Zertifizierung in der hier vorgeschlagenen Form derzeit noch nicht

---

103 *Marburger*, in: Rüthers/Stern 1984, 285.
104 Zum Cloud Computing s. *Roßnagel*, in: ders. 2015, 239.
105 *Roßnagel*, in: Bäumler/v. Mutius 2002, 116.
106 *Wegenroth*, in: Hof/Wengenroth 2007, 1.
107 *Schefzig*, ZD 2015, 503.

gibt, wird die Rechtsordnung daraufhin zu untersuchen sein, welche Vorgaben de lege lata und de lege ferenda für ein solches System relevant sind.

Bei dieser Analyse wird der Bedeutungsgehalt einschlägiger Rechtsnormen durch Auslegung gemäß allgemeiner Auslegungsmethoden[108] ermittelt und auf das Beispiel Cloud Computing und dessen Zertifizierung angewendet. Die anschließende Entwicklung des dynamischen Zertifizierungssystems erfolgt anhand der Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen (KORA).[109] Mit dem Ziel besonders vorteilhafter, das heißt rechtsverträglicher Gestaltung, schafft KORA über ein stufenweises Vorgehen die Verbindung zwischen den zunächst inkompatibel erscheinenden Disziplinen Recht und Technik.

Im Zentrum der Betrachtungen liegt das Datenschutzrecht. Dabei sind urheberrechtliche, kartellrechtliche, strafrechtliche und strafprozessuale Aspekte ebenso ausgeklammert, wie Fragen der Vertragsgestaltung. Das Datenschutzrecht selbst ist abzugrenzen vom Schutz der kognitiven Aspekte des Eigentums, die Gegenstand des Immaterialgüterrechts sind.[110] Auch ist Datenschutzrecht nicht zu verwechseln mit dem Schutz von Datenbanken in § 87a UrhG und von Datenbankwerken in § 4 UrhG, bei denen es jeweils nicht um den Schutz des einzelnen Datums geht, sondern in erster Linie um das Schema der Datenbank und der systematischen oder methodischen Anordnung der einzelnen Elemente, wobei für Datenbankwerke nach § 4 UrhG sogar eine eigene geistig-schöpferische Leistung erforderlich ist.[111] Abzugrenzen ist das Datenschutzrecht ferner vom Wirtschaftsrecht im engeren Sinne. Als digitaler Inhalt[112] sind Daten mittlerweile anerkann-

---

108 Während nationale Normen historisch, teleologisch, grammatikalisch und systematisch auszulegen sind, müssen Unionsrechtsakte autonom und anhand der Auslegungsmethoden ausgelegt werden, die der Europäische Gerichtshof angewandt hat.

109 Die Methode geht auf die *Projektgruppe verfassungsverträgliche Technikgestaltung (provet)* zurück, die sie an verschiedenen Forschungsprojekten rechtlicher Gestaltung angewendet und erprobt hat. Zu nennen ist z.B. die Gestaltung von ISDN-Anlagen (*Hammer/Pordesch/Roßnagel* 1993, 43ff.).

110 Etwa das Urheber-, Patent-, Markenrecht und das Recht verwandter Schutzrechte.

111 *Dreier*, in: Dreier/Schulze 2015, § 4 UrhG, Rn. 1 sowie § 87a UrhG, Rn. 4ff.

112 Vgl. Art. 2 Nr. 11 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25.10. 2011 über die Rechte der Verbraucher, ABl. EU 2011, L 304, 64; Eg. 19 definiert „Digitale Inhalte" darüber hinaus als „Daten, die in digitaler Form hergestellt und bereitgestellt werden, wie etwa Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte, unabhängig

tes Wirtschaftsgut[113] und kaufrechtlich schützenswert.[114] Diese Aspekte werden nicht Gegenstand der Untersuchung sein.

Es besteht insoweit eine Forschungslücke, da zwar Cloud Computing aus datenschutzrechtlicher Sicht untersucht wurde[115] und auch das Zertifizierungsverfahren vor Geltung der Datenschutz-Grundverordnung Gegenstand von Untersuchungen war.[116] Daneben finden sich Forschungsarbeiten, die für das dynamische Zertifizierungsverfahren allenfalls am Rande von Bedeutung sein werden.[117] Im Wesentlichen unerforscht sind bisher allerdings sowohl die datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung als auch ein dynamisches Zertifizierungsverfahren auf deren Grundlage. Es existiert insbesondere keine Hinführung allgemeiner rechtlicher Probleme zu der konkreten Frage der dynamischen Zertifizierung.

Die Forschungsarbeit entstand zu großen Teilen im Rahmen der Mitarbeit in dem interdisziplinären Forschungsprojekt „Next Generation Certification" (NGCert), gefördert durch das Bundesministerium für Bildung und Forschung (BMBF). Das NGCert-Konsortium unter der Leitung des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC) bestand neben der Universität Kassel aus der Technischen Universität

---

davon, ob auf sie durch Herunterladen oder Herunterladen in Echtzeit (Streaming), von einem körperlichen Datenträger oder in sonstiger Weise zugegriffen wird.".

113 Vgl. die UsedSoft-Entscheidung des EuGH und diesem folgend des BGH, bei denen es in erster Linie um die Erschöpfung beim Softwarekauf ging, die aber einem Nutzer endgültig übertragene Daten als verkehrsfähiges Gut anerkannt haben (vgl. Urt. V. 3. Juli 2012 – C-128/11, ECLI:EU:C:2012:407, Rn. 61 – UsedSoft/Oracle, bzw. BGH, NJW-RR 2014, 360ff.).

114 Vgl. Art. 2 lit. j sowie Art. 5 des Entwurfs der EU-Kommission und des Rates über ein Gemeinsames Europäisches Kaufrecht vom 11.10.2011, KOM(2011) 635 endgültig.

115 Bspw. *Bedner* 2013; *Brennscheidt* 2013; *Kroschwald* 2015. In Fachartikeln wird gelegentlich die Kontrollpflicht des Auftraggebers angesprochen, jedoch keiner ausführlichen Analyse zugeführt. Für ein Datenschutzaudit plädiert bspw. *Selzer*, DuD 2013, 215 ff.

116 Etwa *Bieback* 2008. Weitere Untersuchungen zu Fragen der Zertifizierung von IT-Sicherheit sind eher technisch orientiert und gehen nicht ausreichend auf rechtswissenschaftliche Fragestellungen ein, wie etwa *Rannenberg* 1998.

117 Mit der Frage des Vertrauens in Mobile Commerce befasst sich beispielsweise die rechtswissenschaftliche Arbeit von *Jandt, dies.* 2008; *Brönneke* analysiert das Zusammenspiel von Transparenz und Vertrauen, *ders.*, in: Klumpp u.a. 2008, 301ff.; Fragen rechtlicher Behandlung von Automatisierbarkeit von Prüfungsschritten behandelt *Boos*, *dies.* 2015.

München, der Universität zu Köln, der Universität Passau und Partnern aus der Wirtschaft, namentlich Fujitsu und dem EuroCloud Deutschland_eco e.V.

1.4 Gang der Untersuchung

Bevor die aufgeworfenen Fragen geklärt und ein Konzept dynamischer Zertifizierung entwickelt werden können, müssen die tatsächlichen Gegebenheiten und normativen Rahmenbedingungen untersucht werden. Zunächst behandelt das zweite Kapitel Cloud Computing in tatsächlicher Hinsicht, dessen Dienste dynamisch zertifiziert werden sollen.

Das dritte Kapitel beantwortet cloudrelevante Rechtsfragen. Von Bedeutung für ein Konzept dynamischer Zertifizierung sind die durch die Verwendung von Cloud Computing möglicherweise betroffenen Grundrechte. Die Analyse der zugrundeliegenden Grundrechte verdeutlicht, dass bei der Nutzung von Cloud Computing datenschutz-, datensicherheits- und geheimnisschutzrechtliche Aspekte vorrangige Bedeutung einnehmen.

Das vierte Kapitel untersucht herkömmliche datenschutz- und datensicherheitsrechtliche Zertifizierungsverfahren im Zusammenhang mit Cloud Computing-Diensten. Dazu werden tatsächliche Konzepte abstrakt analysiert und Begriffe voneinander abgegrenzt.

Im fünften Kapitel werden zertifizierungsrelevante Rechtsfragen beleuchtet. Insbesondere werden die Anforderungen der Datenschutz-Grundverordnung an ein datenschutzrechtliches Zertifizierungsverfahren sowie Fragen der Werbung mit einem Zertifikat und deren lauterkeitsrechtliche Implikationen untersucht. Auf dieser Grundlage werden Schwächen herkömmlicher, das heißt nichtdynamischer Zertifizierungsverfahren, herausgestellt.

Ein sechstes Kapitel bewertet den Aspekt der Dynamik des Zertifizierungsverfahrens. Dabei wird Dynamik als Ausgleich existierender Schwächen und zur Förderung von Vertrauen untersucht. Ergebnis dieses Kapitels sind regulativ sowie organisatorisch auszugleichende Schwächen eines dynamischen Verfahrens und Grenzen, auf die ein solches Verfahren stößt.

Das siebte Kapitel dient der Entwicklung eines rechtsverträglichen dynamischen Zertifizierungsverfahrens von Cloud Computing-Diensten anhand der gewonnenen Ergebnisse, das selbst wiederum als Cloud-Dienst erbracht wird. Ein bewährtes methodisches Vorgehen sorgt dabei für Nachvollziehbarkeit und rechtfertigt damit die Festlegung bestimmter technischer Gestaltungsziele als zwingend oder lediglich als Empfehlung.

Im achten Kapitel wird die technikkonforme Rechtsfortbildung behandelt. Darin werden Regelungsdefizite ausgemacht, die sich aus der Datenschutz-Grundverordnung für Zertifizierungen ergeben und entsprechende Empfehlungen ausgesprochen, die sich gemäß der Kompetenzverteilung an die verschiedenen möglichen Regelungsgeber richten.

Ein neuntes Kapitel fasst die Ergebnisse zusammen.

2 Grundlagen des Cloud Computing

Die Entwicklung eines Konzepts zur dynamischen datenschutz- und datensicherheitsrechtlichen Zertifizierung von Cloud-Diensten erfordert zunächst einige Klarstellungen hinsichtlich des Prüfungsgegenstands.

Darstellungen zum Cloud Computing lassen sich zuhauf finden.[118] Es ist nicht beabsichtigt dieser Fülle einen weiteren Definitionsversuch hinzuzufügen. Vielmehr stellt Cloud Computing für diese Untersuchung lediglich einen Anwendungsfall dar, anhand dessen das dynamische Zertifizierungsverfahren entwickelt werden soll. Seine ausführliche Darstellung verbietet sich deshalb ebenso wie eine abschließende Betrachtung und Entscheidung der vorherrschenden rechtlichen Streitfragen rund um das Cloud Computing.[119]

2.1 Definition

Eine einheitliche Definition des Cloud Computing gibt es nicht. Am weitesten verbreitet scheint jedoch der folgende Ansatz des dem US-amerikanischen Handelsministerium unterstellten Standardisierungs- und Technologieinstituts[120] zu sein:[121]

> „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[122]

Nach einer Weiterentwicklung der Definition durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet Cloud Computing

---

118 Vgl. Bspw. NIST, SP 800-146; *Catteddu/Hogben* ENISA Cloud Computing 2009, passim.

119 S. im Einzelnen zu den rechtlichen Fragen unter 3. sowie *Kroschwald* 2016, passim; *Barnitzke* 2014, passim; Hilber 2014, passim; Roßnagel 2015, passim; *Kaulartz* 2016, passim; Artikel 29-Datenschutzgruppe, WP 196, 6.

120 National Institute of Standards and Technology (NIST).

121 So auch *Schneider/Sunyaev* 2015, 5.

122 NIST, SP 800-145, 2.

> „das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software."[123]

Art. 4 Nr. 19 der Cybersicherheitsrichtlinie[124] verfolgt hingegen ein sehr weites Begriffsverständnis. Danach ist ein Cloud Computing-Dienst ein digitaler Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht. Dieses Begriffsverständnis ist nicht frei von Kritik,[125] wird aber dennoch dieser Untersuchung zugrunde liegen, da es entwicklungsoffen gefasst ist und damit dem Sinn und Zweck des Untersuchungsgegenstands am ehesten entspricht.

Die Eigenschaften des Cloud Computing lassen sich wie folgt zusammenfassen:

- Virtualisierung,[126]
- Mehrmandantenfähigkeit durch Ressourcenbündelung,[127]
- Skalierbarkeit,[128]

---

123 BSI, Cloud Computing Grundlagen, abrufbar auf dem Internetauftritt des BSI unter www.bsi.bund.de, zuletzt abgerufen am 15.3.2019.

124 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Abl. EU 2016, L 194,1, fortan „Cybersicherheitsrichtlinie" oder „NIS-RL".

125 *Schallbruch* kritisiert, dass die Definition unscharf sei und bei fortschreitender Virtualisierung von Informationstechnik sukzessive weitere Dienste erfasse (vgl. *Schallbruch*, CR 2016, 666).

126 Der Begriff der Virtualisierung umschreibt „Methoden, die eine künstlichen Sicht auf Ressourcen eines Computers erlauben" (*Lehmann/Giedke*, CR 2013, 611). Das heißt, dass Hard- und Software voneinander entkoppelt und auf einer Hardwarelandschaft virtuelle Strukturen betrieben werden können, die voneinander abschirmbar und miteinander vernetzbar sind (vgl. *Pohle/Ammann*, CR 2009, 274); s.a. *Lenzer*, in: Conrad/Grützmacher 2014, § 9 Rn. 27ff.

127 Als Mandant wird in diesem Zusammenhang ein oder mehrere Cloud-Nutzer verstanden, die sich den Zugriff auf eine Menge virtueller oder physikalischer Ressourcen teilen (s. z.B. DIN ISO/IEC 17788:2016, Nr. 3.2.37); zur Ressourcenbündelung vgl. *Schneider/Sunyaev* 2015, 6.

128 Skalierbarkeit bedeutet, dass Ressourcen je nach Bedarf flexibel erweitert oder reduziert werden können (vgl. dazu *Schneider/Sunyaev* 2015, 6; *Krcmar* 2015, 723).

- bedarfsgerechter Zugriff durch service-orientierte Architektur,[129]
- verbrauchsorientierte Vergütungsmodelle[130] und
- Netzwerkanbindung.[131]

2.2 Beteiligte

Am Cloud Computing sind im Wesentlichen die betroffene Person,[132] das heißt eine lebende natürliche Person, deren personenbezogene Daten verarbeitet werden, der Cloud-Kunde und der Cloud-Anbieter beteiligt.

Der Cloud-Kunde ist die Partei, die auf rechtsgeschäftlicher Grundlage Cloud-Dienste nutzt. Er kann eine juristische Person oder eine Personenvereinigung sein. Ist er hingegen eine natürliche Person, ist er zugleich betroffene Person, soweit er seine eigenen Daten in die Cloud-Umgebung überträgt. Sollte er Daten eines anderen in die Cloud übertragen, ist jener (ebenfalls) betroffene Person.

In Abgrenzung zum Cloud-Kunden ist der Cloud-Dienstleistungsnutzer (Cloud-Nutzer) derjenige, der den Cloud-Dienst anwendet. Cloud-Kunde und -Nutzer können in einer Person zusammenfallen. Allerdings kann der Cloud-Nutzer auch der Kunde[133] des Cloud-Kunden, dessen Mitarbeiter oder die betroffene Person selbst sein. Folglich ist der Cloud-Nutzer regelmäßig eine natürliche Person.[134]

---

129 Nutzer können selbstständig auf Ressourcen zugreifen und Leistungsparameter beinahe unmittelbar anpassen (*Schneider/Sunyaev* 2015, 6).

130 Vgl. *Schneider/Sunyaev* 2015, 6.

131 Das gilt für die öffentliche Cloud, nicht unbedingt für die private Cloud (vgl. *Schneider/Sunyaev* 2015, 6); s. zu den Eigenschaften auch *Lins/Sunyaev*, in: Krcmar u.a. 2018, 8f.

132 Das ist gemäß Art. 4 Nr. 1 DSGVO eine identifizierte oder identifizierbare natürliche Person; s. im Einzelnen unter 3.3.2.2.2.1.

133 Es können dem Cloud-Kunden beliebig viele weitere Kunden nachgeschaltet sein. Der Begriff des „Kunden" ist hier im Sinne eines Endkunden zu begreifen.

134 Nach DIN ISO/IEC 1788:2016, Nr. 3.2.17 kann der Cloud-Nutzer zudem eine mit dem Cloud-Kunden verbundene Entität, wie etwa ein Gerät oder eine Anwendung sein. Dieser Fall kann allerdings für die Zwecke dieser Untersuchung außer Acht bleiben, da der Cloud-Nutzer nur dann datenschutzrechtlich von Bedeutung sein kann, wenn er selbst betroffene Person ist, dessen personenbezogene Daten bei der Nutzung des Cloud-Dienstes entstehen können.