# Internet der Zukunft

## Ein Memorandum

Christopher Jones
Ralf Nobis
Susanne Röchner
Paul Thal

2010

# Inhaltsverzeichnis

# Über die Autoren

**Christopher Jones**, LL.M. Eur., ist nach seinem Studium der Rechtswissenschaft seit 2008 wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik (Prof. Hilgendorf) und promoviert im Bereich des Internetstrafrechts. Sein Forschungsschwerpunkt liegt bei neuen Phänomenen im Web 2.0, insbesondere dem Cloud-Computing.

**Ralf Nobis** ist seit dem Wintersemester 2006/07 Student der Rechtswissenschaft und des Europäischen Rechts an der Julius-Maximilians-Universität Würzburg und war in der Zeit von 2008 bis 2010 als studentische Hilfskraft am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik (Prof. Hilgendorf) tätig.

**Susanne Röchner** war nach ihrem Studium der Rechtswissenschaften und dem Europäischen Recht in der Zeit von Juli 2009 bis April 2010 als wissenschaftliche Hilfskraft am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik (Prof. Hilgendorf) tätig und promoviert im Bereich des Familienrechts (bei Prof. Scherer, Professur für Bürgerliches Recht und Zivilprozessrecht).

**Paul Thal**, ist nach seinem Studium der Rechtswissenschaft und dem Europäischen Recht seit 2009 wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik (Prof. Hilgendorf) und promoviert im Bereich des materiellen Strafrechts. Zu seinen Forschungsschwerpunkten zählen das Computer- und Internetstrafrecht sowie aktuelle Fragen zur strafrechtlichen Einwilligung.

# Teil 1: Einleitung

Wie kaum eine andere technische Neuerung hat das Internet das tägliche Leben von Millionen von Menschen verändert. Quasi im Gegenzug verändern mittlerweile aber auch Millionen von Menschen ihrerseits das Internet. Aus dem einfachen User wurde der Creator. Diese Entwicklung wird vielerorts unter den Begriff des Web 2.0 gefasst, das vor allem als Schlagwort die veränderte Rollenverteilung im Web beschreibt. Das Web 2.0 lässt sich aber auch typologisch begreifen, als Zusammenfassung vieler Einzelphänomene, die den Typus Web 2.0 charakterisieren. Diese Phänomene befinden sich aber (wie auch das Web selbst) in einem stetigen Wandel und Weiterentwicklungsprozess, sodass sie sowohl dem Web 2.0 als auch dem Internet der Zukunft zugehörig zu sein scheinen:

Während die Potentiale des Cloud Computing und der Augmented Reality wohl noch in den Kinderschuhen stecken, haben soziale Netzwerke, ubiquitäres Computing und Mashups die Medienlandschaft bereits grundlegend verändert. Eine stetige technische und ökonomische Weiterentwicklung dieser Phänomene kann allerdings nur auf den geleiteten Bahnen des Rechts stattfinden. Fraglich ist aber gerade – wie es im Bereich der neuen Medien so oft der Fall ist -, ob das Recht über die nötigen Rahmenbedingungen verfügt, um den besagten Entwicklungen entgegenzutreten. Das Memorandum Internet der Zukunft zeigt diese rechtlichen Hintergründe für die wichtigsten aktuellen IT-Erscheinungen auf und beleuchtet die besagten Phänomene aus technischer und ökonomischer Sicht, was letztlich auch dem interdisziplinären Charakter der Rechtsinformatik Rechnung trägt.

# Teil 2: Wirtschaftliche Grundlagen des Web 2.0

*R. Nobis*

## Kapitel 1: Einführung

Circa 40 Millionen Deutsche nutzen regelmäßig das Internet. Dennoch kennen gerade einmal nur ein Drittel der Internetnutzer den Begriff „Web 2.0“ oder das, was sich hinter diesem Begriff verbirgt. In diesem Bereich geht es in erster Linie um den Menschen. Der Internetnutzer surft im Zeitalter des Web 2.0 nicht mehr nur durch das Internet. Vielmehr verändern und bereichern die User das Webgeschehen. Mit dem Web 2.0 erobern sich die Nutzer das Internet und erhalten Möglichkeiten, das Web aktiv mitzugestalten. Denn nie war es einfacher, Texte, Fotos oder Videos auf Internetplattformen zu veröffentlichen.[1]

Aber woher stammt die Bezeichnung „Web 2.0“? Der Begriff ist das Ergebnis eines Brainstormings zwischen Tim O’Reilly und Dale Dougherty aus dem Jahr 2004.[2] O’Reilly, Dougherty sowie weitere Internet-Pioniere hatten festgestellt, dass trotz des wirtschaftlichen Crashs im Jahr 2001, als die Dotcom-Blase platzte, das Internet wichtiger denn jemals zuvor sei und dass diejenigen Webseiten, die das Dotcom-Desaster überlebt hatten, insbesondere inhaltlich und konzeptionell einige besondere Gemeinsamkeiten aufwiesen. Hieraus Erkenntnis ziehend, definierten sie den Börsencrash im Herbst 2001 als einen Wendepunkt für das Internet und bezeichneten das hieraus hervorgegangene Web als „Web 2.0“.[3] Somit postuliert dieser Begriff eine neue Generation des Webs; eine Weiterentwicklung von statischen zu dynamischen Webseiten.[4]

Mit der Veränderung des Internets hin zu einem Web 2.0 wird das World Wide Web zu einem Netz von Menschen. Soziale Netzwerke wie Facebook oder die VZ-Netzwerke aber auch reine Tauschplattformen wie bspw. Flickr ermöglichen den direkten Kontakt zwischen den Usern. Hierbei spielt es keine Rolle, an welchem

[1] *Beck*, Web 2.0: Konzepte, Technologie, Anwendungen, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 8.

[2] *Hippner*, Bedeutung, Anwendungen und Einsatzpotenziale von Social Software, in: Hildebrand/Hofmann (Hrsg.), Social Software, HMD Heft 252, Dezember 2006, S. 6.

[3] *Lange*, Web 2.0 zum Mitmachen, 2007, S. 6 (ftp://ftp.oreilly.de/pub/katalog/web20_broschuere.pdf).

[4] Dennoch ist der Begriff auch umstritten. So wird er bspw. von Tim Berners-Lee, dem Begründer des World Wide Web, kritisch gesehen.

Computer sich der Einzelne gerade befindet. E-Mail, Weblogs, Wikis und Bookmarks sind überall erreichbar.

Das Web 2.0 baut somit dem Grunde nach auf der Partizipation der Internetnutzer auf. Im weitesten Sinne ist es die Verknüpfung von nutzerbasierten Angeboten zu einer aktiven Nutzungsform des World Wide Web.[5] Hintergrund hierfür ist eine veränderte Nutzung und Wahrnehmung des Internets.[6] Immer mehr Internetangebote laden zum Mitmachen ein. Die Benutzer erstellen, bearbeiten und verteilen Inhalte in quantitativ und qualitativ entscheidendem Maße selbst, unterstützt von interaktiven Anwendungen.[7] Der User ist gleichzeitig Informationskonsument und -produzent. „Nutzer generieren Mehrwert", bezeichnet Tim O'Reilly diesen Wandel.[8] Das Web 2.0 bestimmt die interaktiven Kommunikationsmöglichkeiten in der Weise neu, dass die Inhalte nicht mehr nur von bestimmten Unternehmen zentralisiert bearbeitet und über das Internet zur Verfügung gestellt bzw. verbreitet werden, sondern darüber hinaus und insbesondere von einer Vielzahl von Nutzern, die sich mit Hilfe sozialer Software untereinander verbinden, sog. „User Generated-Content"[9].[10]

Fraglich ist nun, wie Internet-Start-up-Unternehmen als auch etablierte Unternehmen, die einen Einstieg in die Welt des Web 2.0 planen, diese Weiterentwicklung für sich nutzen können. Denn mittlerweile ist generell deutlich geworden, dass das „soziale Web" auch wirtschaftlich eine enorme Relevanz aufweist. An dieser Stelle sollten die Unternehmen und vor allem die Firmen, die sich neu gründen und von den ökonomischen Vorzügen des Web 2.0 Kapital erhoffen (sog. „Startupper") den starken Partizipationswillen der Internetuser nutzen.[11] Bereits der Internetpio-

---

[5] *Knappe/Kracklauer*, Verkaufschance Web 2.0. Dialoge fördern, Absätze steigern, neue Märkte erschließen, 2007, S. 18.

[6] http://de.wikipedia.org/wiki/Web_2.0.

[7] Vgl. hierzu auch *Beck*, Web 2.0: Konzepte, Technologie, Anwendungen, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 4.

[8] *Lange*, Web 2.0 zum Mitmachen, 2007, S. 3 (ftp://ftp.oreilly.de/pub/katalog/web20_broschuere.pdf).

[9] Zum Begriff des sog. „User-Generated-Content" vgl. *Karla*, Implementierung von Regelungskreisen in Geschäftsmodellen für Web 2.0-Publikumsdienste, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 21.

[10] In diesem Zusammenhang ist es klar erkennbar, wie wichtig die technische Entwicklung war. Durch die Einführung von Bandbreitverbindungen (DSL), in dessen Rahmen das Internet zum Massenprodukt avancierte, war auch die Nutzung hochwertigen Contents, wie Musik oder Videos möglich und die Voraussetzungen für eine Bereitschaft zur aktiven Partizipation im Web 2.0 geschaffen worden.

[11] *Beck*, Web 2.0: Konzepte, Technologie, Anwendungen, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, 8 f.

nier Robert Metcalfe hat gesagt, dass der Wert eines Netzwerks mit der Zahl seiner Nutzer exponentiell steige.[12] Das vielumfassende, größtenteils kostenfreie Webangebot mit zahlreichen Möglichkeiten zur Generierung von „User-Generatet-Content" zieht millionenfach die Internetnutzer an. Für Web 2.0-Unternehmen gilt daher der Grundsatz, dass die erfolgreichsten Webangebote die sind, in denen der User selbst für die Inhalte sorgt. Dies gilt es adäquat umzusetzen. Das bedeutet, dass die Nutzbarmachung der kollektiven Intelligenz im Web 2.0 die herausragende Chance darstellt, als Unternehmen gewinnbringend zu agieren. Ein enorm wichtiger Faktor ist in diesem Zusammenhang, dass der einzelne User nicht nur Content generiert, sondern darüber hinaus automatisch auch dessen Weiterentwicklung betreibt.

Dennoch bilden sich im Rahmen der ökonomischen Betrachtungsweise in diesem Zusammenhang auch Probleme, die ein profitables Wirtschaften im Web 2.0 stark erschweren können. Zwar ziehen Web 2.0 Anwendungen einen sehr großen Kreis von Internetznutzern an, doch sind viele Plattformen und Dienste kosten- und werbefrei. Beachtet man, dass auf der anderen Seite enorme Programmierungs-, Pflege- und Traffickosten anfallen, wird ein Wirtschaften ohne unterstützende Investitionen sehr erschwert. Daher sollten die unter dem Punkt II. dargestellten ökonomischen Erfolgsfaktoren Beachtung finden.

Nichtsdestotrotz konnte in den letzten Jahren weltweit eine massive Akquisitionswelle in der Internetbranche beobachtet werden.[13] Hierbei lag das Investitionsinteresse primär auf den neuen Web 2.0-Plattformen. Beispielsweise erwarb das Online-Auktionshaus eBay für 630 Millionen Dollar die Preisvergleichsseite shopping.com und für 2,5 Milliarden Dollar das Internettelefonunternehmen Skype. Google eignete sich für 1,6 Milliarden Dollar die Videoseite YouTube an.[14] Vor dem Hintergrund dieser Entwicklung und der Bedeutung der Kapitalgenerierung im Web 2.0 kommt der Analyse der möglichen Geschäftsmodelle eine äußerst hohe Relevanz zu. Unter dem Punkt III. soll daher eine Klassifikation der im Web 2.0 anwendbaren Geschäftsmodelle erfolgen.

---

[12] *Lange*, Web 2.0 zum Mitmachen, 2007, S. 8 (ftp://ftp.oreilly.de/pub/katalog/web20_broschuere.pdf).

[13] Siehe die Ausführungen von *Wirtz/Ullrich*, Geschäftsmodelle im Web 2.0, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 20 und *Knappe/Kracklauer*, Verkaufschance Web 2.0. Dialoge fördern, Absätze steigern, neue Märkte erschließen, 2007, S. 15

[14] http://www.zeit.de/online/2006/41/google-tube?page=all.

## Kapitel 2: Ökonomische Erfolgsfaktoren

Um das Web 2.0 unternehmerisch erfolgreich nutzen zu können, bedarf es der Beachtung einiger wesentlicher wirtschaftlicher Erfolgsfaktoren. Sie stellen strukturelle und strategische Markteintrittsbarrieren[15] dar, die es zu überwinden gilt.

### *I. Netzwerkeffekte*

Ein sehr bedeutender Erfolgsindikator liegt in den zu erzielenden Netzwerkeffekten. Unter einem Netzwerkeffekt ist eine positive externe Auswirkung zu verstehen.[16] Er beschreibt, dass der Nutzen an einem Netzwerk wächst, sobald dessen Nutzerzahl größer wird. Dies erhöht gleichzeitig den Anreiz für neue Nutzer, dem Netzwerk beizutreten. Im Ergebnis steigt also mit einer zunehmenden Zahl an Netzwerk-Teilnehmern der Nutzen für die Gesamtheit der Teilnehmer exponentiell an.[17] Durch diesen erhöhten Nutzen wird das Netzwerk für noch mehr Personen interessant, die Nutzerzahl wächst weiter an und in der Folge auch der Nutzen für alle.[18] Dieses Phänomen wird allgemein als positive Rückkopplung bezeichnet.[19] Insbesondere im Rahmen von sog. „User-Generated-Content"-Angeboten sind Netzwerkeffekte besonders ausgeprägt.[20]

Bezogen auf die Web 2.0-Plattformen und hierbei insbesondere auf die sozialen Netzwerke bedeutet dies, dass neue Marktteilnehmer es mit gleichen oder inhaltlich ähnlichen Konzepten schwer haben werden, gegen die bereits generierten Netzwerkeffekte der Marktführer wie bspw. die VZ-Netzwerke[21] oder Facebook[22] bestehen zu können. Denn gerade in diesem Marktsegment, in dem viele neue Plattformen online gehen, führen hohe Netzwerkeffekte rasant zu einer Marktdominanz. Im Entstehen begriffene Unternehmen sollten daher von Beginn an auf ein möglichst

---

[15] Vgl. zu den Markteintrittsbarrieren allgemein *Stähler*, Geschäftsmodelle in der digitalen Ökonomie, 2. Auflage 2002, S. 50; *Germer/Wolters/Gell/Pasini*, Geschäftsmodelle und crossmediale Strategien von Web 2.0 Plattformen, 2006, S. 30.

[16] *Dees*, Die Standardisierung des Marketing im internationalen E-Commerce, 2005, S. 23.

[17] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 624; *Stähler*, Geschäftsmodelle in der digitalen Ökonomie, 2. Auflage 2002, S. 227.

[18] Vgl. hierzu *Wirtz/Ullrich*, Geschäftsmodelle im Web 2.0, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 26.

[19] *Wirtz*, Electronic Business, 2. Auflage 2001, S. 277 f.

[20] Vgl. hierzu die Ausführungen in *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 624.

[21] 16 Millionen User europaweit.

[22] 350 Millionen User weltweit.

schnelles Wachstum fokussiert sein, um die zum wirtschaftlichen Überleben nötigen Netzwerkeffekte möglichst zügig erzielen zu können.

### *II. Marke*

Marken sind in den Bereich der strategischen Markteintrittsbarrieren einzuordnen.[23] In weitgehend unerschlossenen Marktsegmenten kann eine starke Marke bei der Generierung von Netzwerkeffekten von großem Nutzen sein[24]. Die Existenz einer ausdrucksvollen Marke ist zudem unabdingbar in Bereichen des Marktes, in dem es bereits eine signifikante Konkurrenz gibt.

Unter dem Begriff der Marke ist ein besonderes, rechtlich geschütztes Zeichen zu verstehen, dass dazu dient, Waren oder Dienstleistungen eines Unternehmens durch eine spezielle Kennzeichnung von Waren und Dienstleistungen anderer Unternehmen zu unterscheiden, die sog. Herkunftsfunktion.[25] Hierdurch können Produkte der eigenen Marke gegenüber der Konkurrenz hervorgehoben werden. Es handelt sich bei einer Marke somit gewissermaßen um eine Visitenkarte, mit der Produkte und Dienstleistungen im Wettbewerbsleben auftreten. In diesem Zusammenhang können Marken für Qualität und Innovation stehen, Emotionen wecken sowie Kaufentscheidungen beeinflussen.

Eine Marke kann beispielsweise durch eine besondere, auf der eigenen Internetpräsenz implizierte Funktion, durch ein besonders nutzerfreundliches Design und gute Benutzbarkeit oder aber auch durch eine die Zielgruppe ansprechende Gestaltung eine geschickte Form des Marketings darstellen. Für ein im Entstehen begriffenes Unternehmen, welches im Rahmen des Web 2.0 wirtschaftlich erfolgreich partizipieren möchte, handelt es sich bei der Generierung einer Marke folglich um ein bedeutungsvolles Instrument. Die Marke erfüllt im Bereich des Internets gegenüber dem User gewichtige Funktionen. So wird das eigene Produkt von der Konkurrenz abgehoben, was dem User als Orientierung dient.[26] Diese Orientierungsfunktion ist insbesondere im Hinblick auf Web 2.0-Plattformen essentiell, die in ein Marktsegment mit signifikanter Konkurrenz eintreten. Der Erfolg mit einer Marke begünstigt

---

[23] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 623.

[24] Vgl. hierzu auch die markenrechtlichen Facetten des Web 2.0-Phänomens „Mashups“ bei *Thal*, in diesem Band, S. 47 ff.

[25] *Fezer*, Kommentar zum Markenrecht, 4. Auflage 2009, § 1, Rdnr. 13.

[26] *Ingerl/Rohnke*, Kommentar zum Markenrecht, 2. Auflage 2003, § 1, Rdnr. 5; *Fezer*, Kommentar zum Markenrecht, 4. Auflage 2009, § 1, Rdnr. 13.

zugleich bei Nutzern das Vertrauen in das Produkt oder die Dienstleistung. Ihr kommt daher eine Selektionsfunktion zu, indem sie dem Internetnutzer eine Auswahl potentiell hochwertiger Angebote aus dem äußerst großen Angebot an Internetmedien gestattet.[27]

Auf der anderen Seite erfüllt die Kommunikation eines gewissen Markengefühls bei den Mitgliedern einer Plattform eine Identifizierungsfunktion. Die Marke trägt daher auch entscheidend zur Kundenbindung bei. Dies darf nicht unterschätzt werden, da insbesondere in der heutigen Zeit die User immer anspruchsvoller und wählerischer werden und nicht davor zurückschrecken einem Unternehmen bzw. einer Plattform den Rücken zuzuwenden. Zusammenfassend stellt die erfolgreiche Generierung einer Marke auf der einen Seite einen weiteren bedeutsamen ökonomischen Erfolgsfaktor für die Etablierung eines Geschäftsmodells im Web 2.0 dar, verkörpert gleichsam auf der anderen Seite auch eine nicht zu unterschätzende Markteintrittsbarriere.[28]

### *III. Technische Anforderungen*

Um ökonomisch erfolgreich zu sein, spielen auch technische Faktoren eine erhebliche Rolle.[29] Hierzu zählen insbesondere die Anforderungen an die Usability, d.h. die durch die User wahrgenommene Benutzerfreundlichkeit einer Internetseite.[30] Usability beschreibt den Bereich, der sich mit der benutzerfreundlichen Gestaltung von interaktiven Produkten beschäftigt. Wird eine Website vom Besucher als nützlich und positiv empfunden, ist sie gegenüber gleichartigen Angeboten deutlich im Vorteil. Kompliziert zu bedienende und unübersichtliche Webseiten werden vom Besucher schnell wieder verlassen und auch vergessen. Sind die Inhalte hingegen gut strukturiert, findet sich der User in der Folge viel einfacher zurecht und ist auch eher bereit, das Webangebot zu nutzen. Ein klarer Aufbau und eine einfache Bedienung der Seite sind daher unabdingbar. Für ein Unternehmen, das auch im Web 2.0 wirtschaftlichen Erfolg anstrebt, kann das Maß an Usability nicht hoch genug sein, wenn es darum geht, die im Internet fokussierten Ziele wie beispielsweise Kunden-

---

[27] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 113, 624 f.

[28] *Dees*, Die Standardisierung des Marketing im internationalen E-Commerce, 2005, S. 77 f.

[29] Vgl. hierzu auch *Beck*, Web 2.0: Konzepte, Technologie, Anwendungen, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 7 f.

[30] Siehe zu den folgenden Ausführungen *Gizycki*, Usability – nutzerfreundliches Web-Design, in: Beier/Gizycki (Hrsg.), Usability – nutzerfreundliches Web-Design, 2002, S. 2 ff.

gewinnung oder Kundenbindung zu erreichen. Eine hohe Usability trägt dazu bei, dass der User die Webseite auch in Zukunft gerne aufruft und wird damit zu einem wichtigen Erfolgsfaktor für den Internetauftritt.

### *IV. Marketing*

Zur Kundengewinnung aber auch zur Kundenbindung stellt das Marketing ein entscheidender Erfolgsfaktor dar. Im Bereich des Web 2.0 gereicht vielen Plattformen, insbesondere den sozialen Netzwerke, zum Vorteil, dass sie ohnehin auf eine kommunikations- bzw. partizipationsfreudige Nutzergruppe abzielen und in hohem Maße auf deren Interaktion setzen. Ein User, der eine Web 2.0-Anwendung nutzt, wird aller Wahrscheinlichkeit nach auch auf anderen, auf Kommunikation und Interaktion basierenden Plattformen online sein und einen gewonnenen positiven Eindruck im Hinblick auf die Promotion einer Webseite von einem anderen online-Medium sogleich durch Mundpropaganda kundtun. Dieses sog. „virale Marketing“ ist eine Form des Marketings, bei dem die Bekanntmachung eines Produktes oder einer Plattform durch positive Mundpropaganda der einzelnen User untereinander erfolgt.[31] Eine anfänglich überraschende oder unerwartete Botschaft verbreitet sich hierbei von Mund zu Mund wie ein Virus. Der Erfolg des viralen Marketings kann, gemessen am grundsätzlich minimalen finanziellen Aufwand, überproportional groß sein. Im Hinblick auf die vielen existierenden Blogs, Chats und Foren lässt sich so in kurzer Zeit eine signifikante Öffentlichkeit erreichen.

Dennoch müssen auch weitere Marketingmaßnahmen in Betracht gezogen werden, da es die Konkurrenzsituation oder die Erreichbarkeit der Zielgruppe unter Umständen erfordert. Schon von Beginn an, d.h. bereits vor und in der Startphase der Gründung einer Web 2.0-Anwendung, ist ein verstärktes Marketing zur Förderung der Bekanntheit von besonderer Bedeutung. Hat das Unternehmen erst einmal Fuß gefasst und Kunden bzw. User gewonnen, ist es im weiteren Verlauf essentiell, dass Maßnahmen zur Kundenbindung erfolgen. Hierbei bieten sich den Unternehmen auch außerhalb des Web 2.0 Möglichkeiten an. Zu nennen sind hier insbesondere das Veranstalten besonderer Partys für Mitglieder der Community oder die Einführung einer Kundenclub-Karte mit verschiedenen monetären oder auch plattformbezogenen Vergünstigungen („Premium-System“).[32]

---

[31] *Thielsch*, Virales Marketing, 2007, S. 6 f; *Langner*, Viral Marketing, 3. Auflage 2009, S. 19, 27.

[32] Vgl. in diesem Zusammenhang auch *Beck*, Web 2.0: Konzepte, Technologie, Anwendungen, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 12; *Wirtz/Ullrich*, Ge-

### *V. Finanzierung*

Die Finanzierung einer Web 2.0-Plattform stellt einer der höchsten Markteintrittsbarrieren dar. Sie stellt sich fast ausnahmslos immer als sehr schwierig und aufwendig dar. In diesem Zusammenhang sollen die auf ein Unternehmen zukommenden Kosten zu Beginn betrachtet werden um hieran anschließend zu erarbeiten, welche Möglichkeiten der Einnahmengenerierung für Unternehmen im Web 2.0 bestehen.

#### *1. Kosten*

Im Hinblick auf die entstehenden Kosten ist zwischen den einmalig anfallenden Fixkosten und den das Unternehmen begleitenden laufenden Kosten zu differenzieren.

Im Medienbereich unterliegen Webseiten bei ihrer Erstellung den zu Beginn anfallenden extrem hohen Fixkosten.[33] Diese fallen insbesondere bei der Programmierung der Plattform an und belaufen sich auf mehrere tausend Euro. Hieran schließen sich die Kosten für das Webdesign und die Konzeption der Webseite an. Darüber hinaus dürfen die Kosten für die Beschaffung der erforderlichen Hardware sowie die Providerkosten nicht zu gering angesetzt werden. Zusätzliche Fixkosten entstehen – neben der Erstellung und Gestaltung von Webinhalten – zudem für die Marktforschung. Schließlich wollen Unternehmen am Markt eine starke Position gewinnen und sich von der Konkurrenz abheben.

Ist eine Webseite erfolgreich programmiert und eingestellt, bleibt zu beachten, dass das Betreiben der Seite weitere, laufende Kosten verursacht. Zum einen benötigt das die Webseite betreibende Unternehmen in technischer und administrativer Hinsicht Personal und Räumlichkeiten. Außerdem fallen unter Umständen Kosten für Lizenzgebühren an. Der größte Kostenfaktor in diesem Bereich stellen hingegen die Providerkosten dar. Hier fallen Ausgaben insbesondere für den Datentransfer („Traffic“) und die Datenbereitstellung („Hosting“) sowie im Marketing – hier ist ebenfalls der Bereich der Marktforschung zu nennen – an.

---

schäftsmodelle im Web 2.0, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 27; *Karla*, Implementierung von Regelungskreisen in Geschäftsmodellen für Web 2.0-Publikumsdienste, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 23.

[33] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 623.

### *2. Einnahmengenerierung*

Vergleicht man die hohen Fixkosten sowie die laufenden Kosten mit den Möglichkeiten der Einnahmenerzielung, ergibt sich ein eher schwieriges Bild. Daher sind insbesondere Start-up-Unternehmen auf jegliche Möglichkeit der Einnahmengewinnung angewiesen. Im Zusammenhang mit einer Unternehmensgründung ist in vielen Fällen auch Hilfe von außen notwendig. So gibt es viele Investoren wie beispielsweise große Fondsgesellschaften oder Konzerne, die auch bereit sind, in neue Web-Projekte zu investieren. Doch trotz solcher Finanzspritzen ist es im Laufe der Zeit für Internetunternehmen erforderlich, auf bestimmte Einnahmequellen zurückzugreifen.

Im Rahmen der Fragestellung, auf welche Art und Weise die Gewinnerzielung stattfinden soll, kann differenziert werden zwischen direkter und indirekter sowie zwischen transaktionsabhängiger und transaktionsunabhängiger Erlösgenerierung.[34]

Mit dem sog. „Paid-Content" gibt es für Unternehmen die Möglichkeit, transaktionsabhängig wie auch transaktionsunabhängig Gewinne zu erzielen.[35] In diesem Zusammenhang wird für einen bestimmten Bereich des angebotenen Inhalts eine Nutzungsgebühr erhoben. Bei den direkt transaktionsabhängigen Nutzungsgebühren erfolgt eine Zahlung bei jeder einzelnen Transaktion wie bei einem Download eines Zeitungsartikels oder eines Musikliedes. Bei den transaktionsunabhängigen Nutzungsgebühren erfolgt die Gewinnerzielung beispielsweise durch das Erheben eines monatlichen Beitrages, die einem über die normalen Angebotsmöglichkeiten hinausgehende Funktionen eröffnet (Premium-Account bzw. Premium-Content).[36]

Nichtsdestotrotz genügt es nicht, ehemals kostenlos verfügbaren Inhalt kostenpflichtig zu offerieren. Der Erfolg im Umgang mit Paid-Content hängt im Wesentlichen von drei Faktoren ab. Zum einen ist die Qualität des kostenpflichtig zur Verfügung gestellten Inhalts wichtig. Der User soll für sein Geld auch etwas erwarten können. Zum anderen spielen die Nutzerfreundlichkeit und die Exklusivität eine

---

[34] Siehe hierzu und zu den folgenden Angaben *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 639 ff. sowie *Wirtz*, Electronic Business, 2. Auflage 2001, S. 214 ff.

[35] *Bohl/Winand*, Unternehmerische Wertschöpfung im Web 2.0, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 32.

[36] *Karla*, Implementierung von Regelungskreisen in Geschäftsmodellen für Web 2.0-Publikumsdienste, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S.20 f.

zentrale Rolle. Der Nutzer soll das Gefühl haben, für die Erhebung von Nutzungsgebühren auch etwas Besonderes zu erhalten. Der Nutzer sollte einen spürbaren Nutzenzuwachs erfahren, so dass er die Kostenpflichtigkeit nicht als negativ, sondern als angemessen empfindet. Im Ergebnis entscheidet die Kundenakzeptanz somit über den Erfolg oder Misserfolg des Paid-Contents.

Als eine weitere Möglichkeit zur Refinanzierung von Webseiten ist die Online-Werbung als eine Form der indirekten transaktionsunabhängigen Form der Erlösgenerierung – und in diesem Zusammenhang insbesondere die Bannerwerbung – zu nennen.[37] Als Bannerwerbung ist eine Werbefläche auf der eigenen Website für ein Drittunternehmen zu begreifen. Der Preis für Bannerwerbung kann sich dabei zum Beispiel nach der Dauer der Werbeschaltung oder nach der Anzahl der Klicks auf den Banner richten.[38]

Die Online-Werbung wurde vor allem in der Vergangenheit als Haupteinnahmequelle genutzt. Jedoch stellt sich in diesem Zusammenhang das Problem, dass eine Webseite eine vergleichbar hohe Anzahl an Benutzern vorweisen muss, um Werbepartner zu gewinnen. Doch um diese hohe Zahl an Nutzer zu erhalten, muss das anbietende Unternehmen hochwertige bzw. exklusive Inhalte veröffentlichen. Hieraus erklärt sich auch die Erforderlichkeit, sich nicht auf einzelne Formen der Einnahmengenerierung zu konzentrieren, sondern eine Mischform, z.B. aus Paid-Content und Online-Werbung, anzustreben.[39] Eine wichtige unternehmerische Entscheidung ist somit die Kombination und die richtige Gewichtung der betreffenden Erlösformen.

Dennoch ist das Schalten von Werbung eine bedeutsame Form der Gewinnerzielung und sollte selbstredend in einer angemessenen Form verwendet werden. Eine Angemessenheit ist jedoch in der Weise wichtig, als dass eine Akzeptanz für einen zu großen Umfang von Werbung bei den Usern fehlt. Die Webseite sollte nicht mit Werbung überfrachtet werden. Im Bereich reiner Web 2.0 Anwendungen sollte sich das Schalten von Werbung als weitestgehend unproblematisch gestalten.

---

[37] *Wirtz*, Electronic Business, 2. Auflage 2001, S. 215.

[38] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 640 f.

[39] *Karla*, Implementierung von Regelungskreisen in Geschäftsmodellen für Web 2.0-Publikumsdienste, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 22; Wirtz, Electronic Business, 2. Auflage 2001, S. 215.

Zwei weitere Erlösmöglichkeiten können zum einen in der sog. „Content-Syndication“ und zum anderen im „Data Mining“ gesehen werden. Unter Content-Syndication wird die Mehrfachverwendung von Inhalten verstanden.[40] Hierbei können eigene Inhalte der Webseite gegen die Zahlung von Lizenzgebühren zur Benutzung an andere Unternehmen weitergegeben werden. Dies ist für Dritte interessant, da sie so Kosten und Personal für die Erzeugung von Webinhalten einsparen können und das Unternehmen, welches den Content zur Verfügung stellt, eine weitere Einnahmequelle erhält. Im Ergebnis werden hierdurch Inhalte verschiedener Webseiten miteinander verbunden.

Data Mining-Erlöse werden durch den Verkauf von Nutzerprofilen an dritte Unternehmen wie z.B. Marktforschungsinstitute erzielt. Nutzerprofile – in diesem Zusammenhang ist insbesondere an Community-Plattformen wie StudiVZ oder Facebook zu denken – enthalten detaillierte Daten über Eigenschaften und Internet-Nutzungsgewohnheiten von Usern.[41] In diesem Zusammenhang ist es selbstverständlich, dass hierunter nicht personenbezogene Daten der User fallen, sondern allgemeine Angaben zu Interessen, Musikgeschmack etc.[42] Aber auch hierbei ist zu beachten, dass für den Verkauf von Userprofilen eine gewisse Größe und gesellschaftliche Relevanz der Plattform oder des sozialen Netzwerks erforderlich ist.[43]

---

[40] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 640.

[41] *Wirtz*, Medien- und Internetmanagement, 2003, 587; *Bohl/Winand*, Unternehmerische Wertschöpfung im Web 2.0, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 27 ff.

[42] Siehe hinsichtlich des großen Missbrauchspotenials im Zusammenhang mit dem Einstellen von personenbezogenen Daten in soziale Netzwerke *Nobis*, in diesem Band, S. 57 ff.

[43] Vgl. in diesem Zusammenhang auch *Bohl/Winand*, Unternehmerische Wertschöpfung im Web 2.0, in: Beck/Mörike/Sauerburger (Hrsg.), Web 2.0, HMD Heft 255, Juni 2007, S. 33.

## Kapitel 3: Geschäftsmodelle

Als Geschäftsmodell wird die Abbildung des Produktions- und Leistungssystems einer Unternehmung bezeichnet. Hierbei wird durch ein Geschäftsmodell in stark vereinfachter Form abgebildet, welche Ressourcen in die Unternehmung einfließen und wie diese durch den innerbetrieblichen Leistungserstellungsprozess in vermarktungsfähige Informationen, Produkte und Dienstleistungen transformiert werden.[44]

Die Auseinandersetzung mit den Geschäftsmodellvarianten im Web 2.0 steht noch am Anfang seiner Entwicklung. Die mannigfaltigen Angebote und die stetige Weiterentwicklung durch viele partizipierenden Internetnutzer erschweren zudem eine genaue Klassifizierung der bestehenden Geschäftsmodelle.[45] Es stellt sich somit die Frage, wie Geschäftsmodelle im Web 2.0 genau aussehen können. Hierzu werden im Folgenden die vier im Internetmanagementbereich bekanntesten Geschäftsmodellvarianten erläutert und eine Verbindung zu möglichen Umsetzungen im Web 2.0 geschaffen.

### *I. Geschäftsmodellklassifikation*

Die Geschäftsmodelle der Internetbranche können auf der Grundlage des 4 C-Modells in die vier Basissegmente Content, Commerce, Context und Connection eingeordnet werden.[46]

---

[44] *Wirtz/Ulrich*, Geschäftsmodelle im Web 2.0 – Erscheinungsformen, Ausgestaltung und Erfolgsfaktoren, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 22; *Stähler*, Geschäftsmodelle in der digitalen Ökonomie, 2. Auflage 2002, S. 40 f.

[45] *Wirtz/Ullrich*, Geschäftsmodelle im Web 2.0, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 22.

[46] *Gräf*, Wie Sie mit Ihrer Website Kunden entwickeln, in: Absatzwirtschaft, Heft 6, 2000, S. 48 ff.

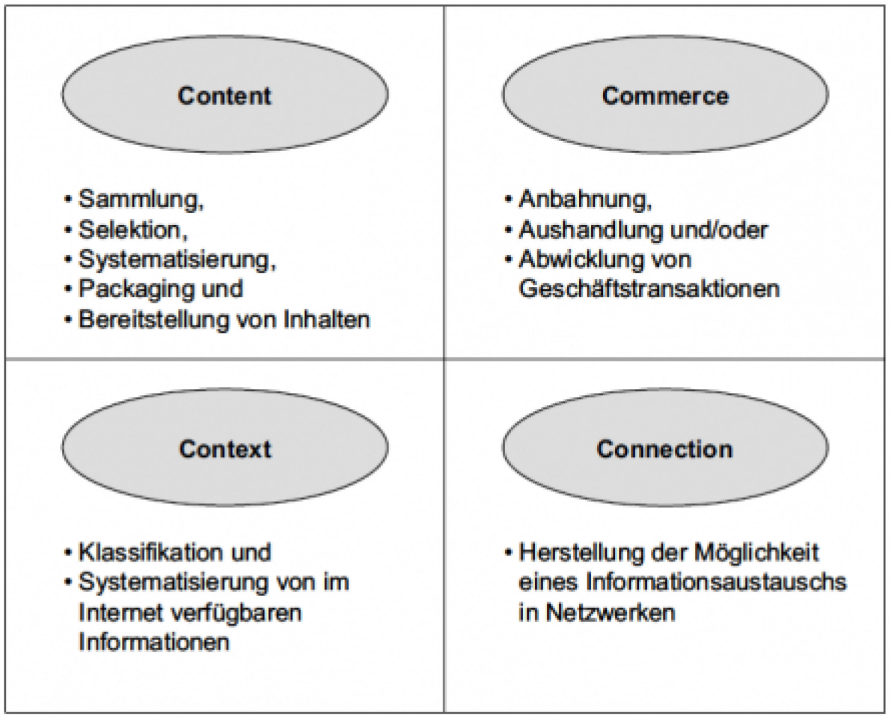


**Abbildung: Geschäftsmodellklassifikation**[47]

### *1. Content*

Das Geschäftsmodellsegment Content zeichnet sich hauptsächlich durch die Bereitstellung digitaler Inhalte über das Internet aus. Ziel des Segments ist es, den Nutzern die Inhalte einfach, bequem, visuell ansprechend aufbereitet und online zur Verfügung zu stellen.[48] Die gesammelten, zusammengefassten und bereitgestellten Informationen können dabei informativer, bildender oder unterhaltender Natur sein. Dementsprechend sind die Geschäftsmodellvarianten E-Information, E-Learning und E-Entertainment sowie E-Infotainment zu unterscheiden.

In den Bereich E-Information sind Plattformen einzuordnen, welche einen vorwiegend informativen Charakter aufweisen. Hierbei können politische, gesellschaftliche oder auch wirtschaftliche Inhalte gesammelt, aufbereitet und bereitgestellt

[47] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 638.
[48] *Wirtz*, Electronic Business, 2. Auflage 2001, S. 219.

werden. Als Beispiele sind hier u.a. der Spiegel[49], wallstreet-online[50] oder die Frankfurter Allgemeine Zeitung[51] zu nennen.

Eine weitere Geschäftsmodellunterkategorie des Segments „Content" stellt das E-Learning dar. Über die alleinige Vermittlung von Informationen hinaus befasst sich das E-Learning mit der digitalen Vermittlung von Lerninhalten. Zudem ist die Verleihung eines Titels bzw. Zertifikates nach der erfolgreichen Erfüllung eines bestimmten Lerninhalts charakteristisch für dieses Modell. Bei den Anbietern für E-Learning existieren neben indirekten, auf Werbemärkten erzielten Erlösformen auch direkte Erlösformen wie beispielsweise Kursgebühren sowie zusätzliche Gebühren für Korrekturen von Tests.[52]

Der Bereich E-Entertainment ist geprägt durch das Angebot von unterhaltenden Inhalten. Hierbei kann eine Unterteilung in E-Games, E-Movies und E-Musik erfolgen. Als Beispiele sind in diesem Bereich Musikload[53] sowie Youtube[54] zu nennen. Die Angebote aus dem Segment E-Infotainment verbinden informierende Inhalte mit unterhaltenden Elementen. Somit stellt dieses Segment eine Hybridform der Bereiche E-Information und E-Entertainment dar.[55]

Im Zusammenhang mit den Entwicklungen durch das Web 2.0 ergeben sich insbesondere im Bereich Content neue Fragestellungen. So gilt es den durch den „User-Generated-Content" produzierten Content entsprechend zu gewichten und in adäquater Weise in den eigenen zur Verfügung gestellten Content zu integrieren. Unternehmen mit entsprechenden Internetplattformen im Segment Content müssen für die Zukunft die Frage berücksichtigen, inwieweit es förderlich ist, zu bestimmten Anteilen von Nutzern generierten Content mit einzubeziehen um die Attraktivität des Angebots zu erhöhen.

[49] www.spiegel.de.
[50] www.wallstreetonline.de.
[51] www.faz.net.
[52] *Wirtz*, Electronic Business, 2. Auflage 2001, S. 226.
[53] www.Musicload.de.
[54] www.youtube.com.
[55] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 645.

### *2. Commerce*

Das Geschäftsmodell Commerce beinhaltet die Anbahnung, Aushandlung und die Abwicklung von Transaktionen im Internet. Das Ziel besteht in der Unterstützung und Ergänzung der traditionellen Phasen einer Transaktion mithilfe des Internets.[56] Das Modell kann hierbei in die Varianten E-Attraction, E-Bargaining/E-Negotiation und E-Transaction unterteilt werden.

Das Teilsegment E-Attraction befasst sich hauptsächlich mit der Anbahnung von Transaktionen. Durch eine inhaltliche Attraktivität der eigenen Präsenz wird eine möglichst hohe Attraktivität auch und gerade für Werbepartner ermöglicht. In diesem Zusammenhang spielen insbesondere Design, Vermarktung, Bewirtschaftung und Vermittlung von Werbeflächen im Internet eine gewichtige Rolle.[57] Hierbei ist insbesondere an die Bannerwerbung zu denken. Im Ergebnis soll eine gewisse Attraktivität für potentielle Werbepartner geschaffen werden, um somit für die Anbahnung einer Transaktion den Boden zu bereiten.

Die Geschäftsmodellvariante E-Bargaining beziehungsweise E-Negotiation beschreibt die Aushandlung der Geschäftsbedingungen. Hierbei fungieren Anbieter dieser Plattformen lediglich als Vermittler zwischen Nutzer und Vertreiber des Produkts. Bei erfolgreicher Vermittlung behalten diese dann z.B. eine Gebühr ein. Eine gesteigerte Partizipation der User ist hier prägendes Merkmal. Zwei sehr bekannte Beispiele in diesem Bereich sind eBay und Myhammer.[58]

Das Teilsegment E-Transaction widmet sich der Abwicklung von Transaktionen im Internet. Im Zusammenhang mit dem Web 2.0 wird vor allem die Zahlungsabwicklung durch neue Möglichkeiten wie PayPal beeinflusst. Hiermit ist sowohl das Versenden als auch das Empfangen von Geld mithilfe des Internets in 65 Ländern möglich.

### *3. Context*

Das Geschäftsmodell Context hat in den letzten Jahren dramatisch an Bedeutung gewonnen. Die Präsenz und die Zunahme erheblicher Mengen an Daten und Informationen im Internet bedingt notwendigerweise die Klassifizierung, Systematisie-

[56] *Wirtz*, Electronic Business, 2. Auflage 2001, S. 230.

[57] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 648.

[58] Vgl. im Zusammenhang mit diesen Beispielen die zugrundeliegende Thematik „Auktion“ und „Price Seeking“ bei *Wirtz*, Electronic Business, 2. Auflage 2001, S. 233.

rung und Selektion dieser Inhalte; dies gilt ohnehin in Zeiten des Web 2.0, in denen der „User-Generated-Content“ einen erheblichen Umfang annimmt. Context-Anbieter wirken als Navigationshilfen und schaffen so eine gewisse Markttransparenz sowie eine Verbesserung der Orientierung für den Nutzer, indem die im Internet verfügbaren Informationen durchsucht und gefiltert werden. Dies erklärt, warum viele Internetnutzer die Internetseiten von Context-Unternehmen – dies sind in erster Linie Suchmaschinen wie Google oder Yahoo – als Startseite festgelegt haben, von der aus Informations- Interaktions- oder Transaktionsangebote anderer Anbieter abgerufen werden.[59]

### *4. Connection*

Hauptmerkmal des Geschäftsmodells Connection ist die Herstellung der Möglichkeit eines Informationsaustausches in Netzwerken. Hierdurch sollen Kommunikationsbarrieren überwunden und eine Interaktion von Nutzern in virtuellen Netzwerken ermöglicht werden. Innerhalb des Geschäftsmodells wird unterschieden zwischen den Segmenten Intra-Connection und Inter-Connection.

Äußerst relevant für den Bereich des Web 2.0 ist das Segement Intra-Connection. Hierbei geht es um die virtuelle Vernetzung von Nutzern durch die Schaffung von Kommunikations- und Austauschplattformen. In diesen Bereich fallen Customer Opinion Portale, dessen Anbieter Nutzern Entscheidungshilfen beim Kauf von Produkten oder Dienstleistungen bereitstellen, indem sie diese bewerten oder durch andere Konsumenten bewerten lassen.[60] Ein Beispiel hierfür ist Ciao.[61]

Eine weitere Gruppe dieser Geschäftsmodellvariante sind Customer Exchanges. Diese Ausprägung des Geschäftsmodells Connection bezeichnet Austauschplattformen von u.a. Musik- oder Videoinhalten. Als Beispiel ist hier das BitTorrent-Netzwerk zu nennen.[62] Der Bereich Inter-Connection schafft den technologischen Zugriff auf das Internet durch sog. Internet Service Provider.

---

[59] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 649 f.
[60] *Wirtz*, Medien- und Internetmanagement, 6. Auflage 2009, S. 652.
[61] www.ciao.de.
[62] www.bittorrent.com.

### *II. Entwicklung durch das Web 2.0*

Die systematische Untersuchung von Geschäftsmodellen im Web 2.0 befindet sich zurzeit noch in einer frühen Phase. Dennoch wurde aufgezeigt, dass die etablierten Geschäftsmodelle geeignet sind, auch die Analyse von unternehmerischen Aktivitäten im Web 2.0 durchzuführen.[63]

Nichtsdestotrotz sind Unternehmen in der digitalen Welt einigen grundlegenden Veränderungen ausgesetzt. Hierzu zählen insbesondere die extrem gesteigerte Partizipationsfreudigkeit und Interaktionsbedürftigkeit der Nutzer. Ausfluss dieses Charakteristikums ist das erhebliche Ausmaß an „User-Generated-Content". Diese Erkenntnisse erklären zugleich die Entwicklung und Anpassungsbedürftigkeit gewichtiger und elementarer Aspekte der Geschäftsmodelle. Zu Beginn des „Electronic Business" wurden die Geschäftsmodelle des 4 C-Modells noch in ihrer Reinform angewandt. Die einzelnen Segmente wurden von Unternehmen getrennt zur Erlösgenerierung genutzt. Eine Vermischung gab es nicht.

Die erheblich wachsende Wettbewerbsintensität aufgrund einer Zunahme der Konkurrenz in der Internetbranche auf der einen Seite und auf der anderen Seite vermehrt durch die gewichtigen Inhalte des Web 2.0, wie der stetig wachsende Partizipationswille der Internetnutzer, führen jedoch dazu, das bestehende Geschäftsmodelle um bislang noch nicht verfolgte Geschäftsmodellvarianten erweitert werden müssen. Unternehmen werden zukünftig ihre Internetpräsenz um Möglichkeiten ergänzen müssen, sodass Internetnutzer kontinuierlich einen Beitrag leisten, in Interaktion mit anderen Nutzern treten und sich mit dem Angebot identifizieren und langfristig integrieren können.[64] Die Anbieter von Web 2.0 Plattformen haben erkannt, ihre Erlösmodelle zu diversifizieren und neue Erlösströme zu erschließen und folglich hierzu die Elemente mehrerer Geschäftsmodelle zu kombinieren. Somit werden die Geschäftsmodelle zunehmend hybrider und multifunktionaler.[65] Ein Beispiel hierfür ist T-Online.[66] Diese Plattform bietet seinen Kunden mit dem Geschäftsmodell Connection nicht nur die Verbindung ins Internet, sondern enthält

---

[63] Zu dem gleichen Schluss gelangen auch Wirz und Ullrich. Siehe hierzu *Wirtz/Ullrich*, Geschäftsmodelle im Web 2.0, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 30.

[64] *Wirtz/Ullrich*, Geschäftsmodelle im Web 2.0, in: Hofmann/Meier (Hrsg.), Webbasierte Geschäftsmodelle, HMD Heft 261, Juni 2008, S. 30.

[65] *Wirtz*, Electronic Business, 2. Auflage 2001, S. 276.

[66] www.t-online.de

durch eine Einkaufsplattform, eine Suchmaschine sowie einem Nachrichtenangebot überdies Elemente aus den Geschäftsmodellen Commerce, Context sowie Content.

## Kapitel 4: Vom Web 2.0 zum Web 3.0 – Das Semantische Web

Wie zu Beginn dieses Beitrages herausgearbeitet, baut das Web 2.0 dem Grunde nach auf dem Partizipations- und Kommunikationswillen der Internetnutzer auf. Das Internet entwickelt sich zu einem „sozialen Web“ und der Nutzer rückt in vielerlei Hinsicht in den Mittelpunkt. Die Internetnutzer können Inhalte produzieren, sich untereinander vernetzen oder über eine Plattform kommunizieren. User generieren eigenen Content und wollen in der Sphäre des Internets aktiv mitwirken und aktiv gestaltend agieren. Dies zeigt sich letztlich nicht nur durch Web 2.0-Medien wie Blogs, soziale Netzwerke oder durch die eindrucksvollste Applikation Wikipedia.

Wie auch die Analyse der in diesem Bereich angewandten Geschäftsmodelle gezeigt hat, wandelt sich das Netz zu einer Plattform, in der der nunmehr aktive Konsument mit einer Vielzahl von Dienstleistungen aus dem Kommunikations-, Informations- und Unterhaltungsbereich interagiert.[67] Unternehmen haben diese Veränderung bereits erkannt und reagiert. Tauschplattformen wie eBay oder Bewertungsportale wie holidaycheck erfreuen sich großer Beliebtheit. Viele Unternehmen werden nachziehen und ihr Angebot den neuen Phänomenen im Internet anpassen.

Doch schon jetzt stellen sich weitere Fragen: Wie sieht die Zukunft aus? Was kommt in der digitalen Welt nach dem Web 2.0? Dieser Materie soll sich im folgenden Kapitel in den Grundzügen gewidmet werden.

Im Zusammenhang mit der Zukunft des Internets ist bereits ein Schlagwort in vieler Munde. Es handelt sich dabei um den Begriff „Web 3.0“. Inhaltlich geht es hierbei um eine Weiterentwicklung des Web 2.0 hin zu einer neuen Entwicklungsstufe, dem sog. „semantischen Web“. Das Web 2.0 ergänzt durch das semantische Netz wird mit dem Begriff Web 3.0 zusammengefasst.[68]

Das semantische Web beruht auf einem Vorschlag von Tim Berners-Lee, dem Erfinder des World Wide Web und stellt eine Erweiterung des World Wide Web dar.[69] Zugleich geht es über das Web 2.0 technisch weit hinaus. Während das World Wide Web einzig und alleine die Funktion hat, sämtliche verfügbaren Daten der Welt mit-

---

[67] Siehe hierzu auch *Knappe/Kracklauer*, Verkaufschance Web 2.0. Dialoge fördern, Absätze steigern, neue Märkte erschließen, 2007, S. 15.

[68] *Tolksdorf*, Web 3.0 – die Dimension der Zukunft (http://www.tagesspiegel.de/zeitung/Sonderthemen;art893,2369841).

[69] *Geisler*, Semantic Web, 2009, S. 15.

einander zu vernetzen, werden durch das semantische Web die Informationen miteinander verknüpft. Ziel ist es, die Bedeutung von Informationen für den Computer verwertbar zu machen.[70] Der Unterschied zum Web 2.0 als stark gesellschaftlich bezogenes Medium stellt in diesem Zusammenhang die Technologiebezogenheit des semantischen Webs dar.

Hintergrund für die Entwicklung des semantischen Webs stellt die immer größer werdende Flut an Informationen dar. Eine Ursache hierfür ist auch im Aspekt des „User-Generated-Content" zu sehen. Die heute schon existierende Datenmasse ist insgesamt zu groß, um von Menschen erfasst und verarbeitet zu werden. Als Lösung für dieses Problem soll das semantische Web herangezogen werden.[71]

Die im Internet verfügbaren Informationen aus den verschiedensten Quellen sollen von Maschinen erfasst, interpretiert und ihrem Sinn nach weiterverarbeitet werden.[72] Ziel ist es, die so erhaltenen Informationen in eine logische Beziehung - sei es inhaltlicher, struktureller oder kontextueller Art – zu setzen und sie miteinander zu verknüpfen um sie so den Menschen nutzbar zu machen, indem das Internet navigierbar wird.[73] Die heute allgegenwärtige Stichwortsuche mithilfe von Suchmaschinen soll insofern weiterentwickelt werden, als das uns das Internet auf eine konkrete Frage hin eine konkrete Antwort geben kann, ohne dass dem eine zeitraubende Suche vorausgeht.[74]

Nichtsdestotrotz kann die digitale Welt des Internets zurzeit ausschließlich von Menschen begriffen werden. Keinem Computer ist es möglich, aus den Daten, die in den Strukturen gewöhnlicher Webseiten inbegriffen sind, direkt Informationen zu gewinnen. Die Entwicklung eines semantischen Webs soll mithin dazu führen, dass die Informationen im World Wide Web von Computern verstanden und verarbeitet werden können.[75] Die Daten in einem semantischen Web sind strukturiert und in ei-

[70] *Geisler*, Semantic Web, 2009, S. 7.

[71] http://de.wikipedia.org/wiki/Semantisches_Web.

[72] *Feigenbaum/Herman u.a.*, Mein Computer versteht mich - allmählich, in: Spektrum der Wissenschaft, November-Ausgabe 2008, S. 93.

[73] *Hitzler/Krötzsch/Rudolph/Sure*, Semantic Web, 2008, S. 11; *Knappe/Kracklauer*, Verkaufschance Web 2.0. Dialoge fördern, Absätze steigern, neue Märkte erschließen, 2007, S. 156.

[74] *Feigenbaum/Herman u.a.*, Mein Computer versteht mich - allmählich, in: Spektrum der Wissenschaft, November-Ausgabe 2008, S. 92; *Geisler*, Semantic Web, 2009, S. 7.

[75] *Ramge*, Mein Computer versteht mich!, Artikel im Semantic Web Company-Portal v. 30.07.2007 (http://www.semanticweb.at/index.php?id=1&subid=57&action=resource&item=1391); *Geisler*, Semantic Web, 2009, S. 16.

ner Form aufbereitet, welche es dem heimischen PC ermöglichen soll, weltweit alle Daten miteinander zu verknüpfen und als eine Einheit zu verarbeiten.[76]

Den Prozess vereinfacht der Umstand, dass die Kommunikationsmöglichkeiten durch das Internet und präziser durch das World Wide Web bereits zur Verfügung gestellt werden. Neu hinzu tritt jedoch die „Sprache" des semantischen Webs, die erforderlich ist, um eine automatische Verarbeitung zu ermöglichen und durch die die Voraussetzungen hierfür geschaffen werden sollen[77] Hier werden spezielle Informations- und Spezifikationssprachen relevant. Die sog. Ontologiesprachen „RDF(S)" und „OWL" sind speziell für die Verwendung im Semantic Web entwickelt worden.[78]

Langfristig soll das semantische Web die Zukunft der digitalen Welt darstellen. Das Wissensmanagement soll einfacher und effizienter gestaltet werden. Welche Anwendungen im semantischen Web jedoch genau möglich werden, ist heute noch nicht zu erblicken.

[76] http://de.wikipedia.org/wiki/Semantisches_Web.

[77] Siehe in diesem Zusammenhang und insbesondere zu den einzelnen Formen der Sprache wie z.B. dem RDF-Format *Feigenbaum/Herman u.a.*, Mein Computer versteht mich - allmählich, in: Spektrum der Wissenschaft, November-Ausgabe 2008, S. 97; *Hitzler/Krötzsch/Rudolph/Sure*, Semantic Web, 2008, S. 91 ff.

[78] *Hitzler/Krötzsch/Rudolph/Sure*, Semantic Web, 2008, S. 12.

# Teil 3: Einzelne Phänomene

## Kapitel 1: Cloud-Computing

*C. Jones*

Cloud-Computing beschreibt eine umfassende IT-Strategie, die immer mehr Verbreitung findet. Im Wesentlichen bedeutet Cloud-Computing, dass Anwendungen, wie etwa Textverarbeitung, Tabellenkalkulation oder Dateiverwaltung, nicht mehr auf dem eigenen PC installiert und geladen werden, sondern „in den Wolken des Internets" ausgeführt werden. Dieser Ansatz unterscheidet sich von „klassischer" IT in einigen wichtigen Punkten, die Besonderheiten des Cloud-Computing führen zu neuen und besonderen rechtlichen Herausforderungen, deren Lösung angesichts der zunehmenden Verbreitung entsprechender Angebote immer wichtiger wird.

### *I. Merkmale des Cloud-Computing*

Das Konzept Cloud-Computing entwickelt bestehende Konzepte wie Grid-Computing, Software as a Service (SaaS), Utility Computing und Virtualisierung[79] weiter, indem es die gesamte IT-Struktur vom privaten oder gewerblichen Endanwender bis zum Server- und Softwareanbieter beschreibt und als Sammelbegriff zusammenfasst.[80] Anwendung findet dieses Konzept bereits heute sowohl für alltägliche Dienste für private Endnutzer, als auch für die Auslagerung ganzer Unternehmensprozesse.

Beispiele für Dienste, die dem Cloud-Computing zugeordnet werden, sind etwa *Amazon Elastic Compute Cloud* (Amazon EC2)[81], *Google App Engine* bzw. *Google Apps Text&Tabellen*[82], *Microsoft Windows Azure*[83], *Zoho Textverarbeitung*, *Apple MobileMe*,

[79] Zur näheren Abgrenzung *BITKOM*, Cloud Computing - Evolution in der Technik, Revolution im Business, 2009, S. 69 ff.; *Söbbing*, MMR 2008, XII; zu verschiedenen Erscheinungsformen *Niemann/Paul*, K&R 2009, 444, 445.

[80] Zur Entwicklung vgl. *Knowledge@W.P.Carey*, Cloud Computing: The Evolution of Software-as-a-Service, http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1614 (Stand: 5.2.2010); *Herrmann*, Grundlagen Cloud Computing, http://www.tecchannel.de/webtechnik/soa/1837978/grundlagen_cloud_computing_saas_virtualisierung/ (Stand: 05.02.2010); *Söbbing*, MMR 2008, XII.

[81] http://aws.amazon.com/ec2/ (20.05.2010). Anwender können hier eigene virtuelle Server mit Datenbanken oder Speicherplatz einrichten oder komplexe Rechenoperationen durchführen lassen.

[82] http://code.google.com/appengine/ bzw. http://docs.google.com (20.05.2010). Google stellt Unternehmen, Privatpersonen und Behörden ein umfangreiches Software-Paket zur umfassenden Kommunikations- und Dokumentenverwaltung zur Verfügung.

[83] http://www.microsoft.com/windowsazure/. Microsoft entwickelt derzeit ein Cloud-Betriebssystem.

*Salesforce* und *GoGrid Cloud Hosting*.[84] Es gibt jedoch unzählige weitere Anbieter, die ähnliche Angebote entwickeln.

Eine einheitliche oder umfassende Definition des Begriffs „Cloud-Computing" besteht indes nicht.[85] Eine klar abgegrenzte Unterscheidung von Cloud-Computing-Anwendungen von anderen IT-Strategien stellt sich angesichts der vielseitigen Einzelaspekte oftmals als unmöglich dar, insbesondere weil IT-Projekte regelmäßig auf einer Vielzahl gemischter und individuell angepasster Lösungen beruhen.[86]

Je nach Schwerpunkt der Betrachtung werden verschiedene Einzelelemente ins Blickfeld gerückt, wobei sich einige Hauptmerkmale des Cloud-Computing identifizieren lassen: Zum einen wird die Cloud-Computing-Anwendung den Benutzern über das Internet oder ein größeres Netzwerk zur Verfügung gestellt. Es findet ein konstanter Datenaustausch zwischen dem Rechner des Benutzers und den Servern des Anbieters statt. Sollte die Verbindung unterbrochen werden, so ist die Anwendung nicht oder nur mit großen Einschränkungen benutzbar. Zum anderen werden auf Seiten des Anbieters Hard- und Softwareressourcen strukturell und physisch getrennt. Der Anbieter kann verschiedene Techniken einsetzen, etwa Virtualisierung oder Clustering, was es ihm erlaubt, die Anwendung für eine Vielzahl an Benutzern gleichzeitig und weltweit zur Verfügung zu stellen. Oft sind die global aufgestellten Rechenzentren des Anbieters untereinander vernetzt und tauschen automatisiert Daten aus – der genaue Ort einer Datenverarbeitung lässt sich kaum oder überhaupt nicht feststellen. Dies unterscheidet Cloud-Computing von klassischer Software, die üblicherweise auf Einzelarbeitsplätzen installiert wird und alle Datenverarbeitungsprozesse nur lokal im eigenen Rechner ausführt.

Im Folgenden wird Cloud-Computing daher als Sammelbegriff für solche Anwendungen verstanden, die Anwenderinterface von Verarbeitungsressourcen trennen und ausschließlich oder im Wesentlichen über ein Netzwerk nutzbar sind, wobei die Verarbeitungsprozesse auf Seiten des Anbieters in einem komplexen, vernetzten Serversystem stattfinden und dem Anwender auf Abruf zur Verfügung stehen.

### *1. Vorteile für den Benutzer*

Auf der Ebene der einzelnen Benutzer bedeutet dies, dass Software, die üblicherweise auf dem eigenen PC installiert, geladen und ausgeführt wird, nun „in der Wolke des

---

[84] Siehe http://www.zoho.com, http://www.apple.com/de/mobileme/, http://www.salesforce.com bzw. http://www.gogrid.com/ (25.05.2010).

[85] *Fickert*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 419.

[86] Ausführlich *Armbrust*, et al., Above the Clouds: A Berkeley View of Cloud Computing, 2009; vgl. *Schuster/Reichl*, CR 2010, 38 ff., die fünf Ebenen des Cloud Computing beschreiben; vgl. zum Stand der technischen Diskussion *Herrmann*, Zum Stand der Diskussion um Cloud Computing, http://www.cio.de/1837978 (Stand: 21.02.2010).

Internets“ bereitgestellt, also auf einem Server ausgeführt wird. Eine lokale Installation entfällt, auch das Betriebssystem des Benutzers spielt kaum mehr eine Rolle. Auch die Hardwareleistungen werden ausgegliedert. Der eigene PC dient lediglich als „Fenster“, durch das auf die Benutzeroberfläche und die jeweiligen Verarbeitungsprozesse des Servers zugegriffen wird. Nur die Eingabemaske, die zu bearbeitenden Daten und Steuerbefehle sowie das jeweilige Verarbeitungsergebnis werden zum Anwender übertragen. Die eigentliche Verarbeitung der Daten, teilweise auch die dauerhafte Speicherung, findet auf den Servern des Anbieters statt, d. h. in dessen (Arbeits-)Speichern und Prozessoren. Deshalb ist die Anwendung – sofern es sich nicht um ein selbständig ablaufendes Programm handelt – ohne Internetzugriff im Wesentlichen nicht nutzbar.

Der Anbieter kann wiederum vorhandene Hard- und Softwareressourcen verschiedenen Kunden gleichzeitig zur Verfügung stellen. Da durch Virtualisierungstechnologien einzelnen Verarbeitungsprozessen keine physikalische Ressource fest zugeordnet wird, kann der Anbieter eine flexible und skalierbare Infrastruktur schaffen.[87]

Ein typisches Anwendungsbeispiel ist etwa ein Textverarbeitungsprogramm. Traditionell wird dieses auf CD-ROM vom Hersteller bezogen und entsprechend der erworbenen Lizenz lokal auf dem PC des Benutzers installiert.[88] Der Benutzer startet die jeweilige Software auf seinem PC, deren Module in den lokalen Arbeitsspeicher geladen werden. Eine entsprechende Benutzeroberfläche wird angezeigt, in der nun lokal gespeicherte Dateien bearbeitet und abgespeichert werden können. Ein Textverarbeitungsprogramm, das als Cloud-Computing-Anwendung entwickelt wurde, ist *Google Text&Tabellen* als Teil der Google AppEngine.[89] Hier registriert sich der Anwender mit seinem Benutzerprofil auf den Webseiten des Anbieters und kann daraufhin über seinen Browser auf eine Onlineanwendung zugreifen, die alle grundlegenden Funktionen eines Textverarbeitungsprogramms bereithält. Die Benutzeroberfläche bildet traditionelle Anwendersoftware nach und lässt sich wie gewohnt per Maus und Tastatur bedienen. Die Übermittlung der Daten an die Anbieterserver geschieht transparent im Hintergrund und wird von Google in deren weltweiten Serverzentren verarbeitet. Für den Anwender macht es hingegen – eine entsprechend schnelle Internetverbindung vorausgesetzt – keinen Unterschied, wo letztendlich die eingegebenen Daten verarbeitet werden.

Das lokal angezeigte Verarbeitungsergebnis einer solchen Web-Anwendung, hier also etwa das formatierte und grafisch gestaltete Textdokument, lässt sich üblicherweise direkt auf der lokalen Festplatte abspeichern. Zusätzlich zur Bereitstellung der Software

---

[87] Zu den Vorteilen im Einzelnen *Schulz/Rosenkranz*, ITRB 2009, 232, 233; *Armbrust*, et al., Above the Clouds: A Berkeley View of Cloud Computing, 2009, S. 1 ff.; *BITKOM*, Cloud Computing - Evolution in der Technik, Revolution im Business, 2009, S. 50.

[88] Etwa Microsoft Word 2007 als Teil von Microsoft Office.

[89] http://docs.google.com; vgl. *Fickert*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 419, 423 f.

bieten viele Anbieter auch die Möglichkeit an, die bearbeiteten Dateien ebenfalls im Online-Speicherplatz zu hinterlegen.[90] Dies bietet dem Anwender, je nach Angebot, zusätzliche Vorteile, etwa die Zugriffsmöglichkeit von jedem PC mit Internetzugang, kontinuierliche Sicherungskopien durch den Anbieter, die einfache Zurverfügungstellung der Daten zur Bearbeitung durch Dritte usw.

### *2. Bedeutung im privaten und geschäftlichen Bereich*

Die tatsächliche und rechtliche Bedeutung dieser IT-Strategie nimmt mit dem Wert und der Wichtigkeit der jeweils ausgelagerten Prozesse zu. Ein einfacher Online-Taschenrechner mag zwar technisch auch als Cloud-Computing-Anwendung ausgestaltet sein, die Relevanz der verarbeiteten Daten dürfte hingegen recht gering sein. Wo aber geschäftliche, geheime oder besondere persönliche Daten gespeichert und verwaltet werden, müssen andere Maßstäbe gelten als dort, wo anonyme Alltagsprozesse verarbeitet werden.

Lagert etwa ein Unternehmen zentrale Verwaltungsprozesse aus, so entsteht ein enges Abhängigkeitsverhältnis zum Anbieter.[91] Soft- oder Hardwareprobleme in lokalen Arbeitsplatzrechnern betreffen üblicherweise nur diesen einen Arbeitsplatz. Installierte Software lässt sich leicht ersetzen. Auf die Server der Public-Cloud-Computing-Anbieter hat der Anwender allerdings regelmäßig keinen direkten Zugriff. Kommt es dort zu Datenausfällen oder technischen Problemen, oder stellt der Betreiber sein Angebot ein, so sind alle Benutzer des Dienstes davon betroffen.

Im geschäftlichen Bereich erfreut sich die Auslagerung von Hard- und Softwareressourcen steigender Beliebtheit, da sich dadurch in vielerlei Hinsicht Kosten und Ressourcen einsparen lassen.[92] Wird Software nicht mehr lokal auf einen PC installiert, muss dieser nicht erst für die Mitarbeiter eingerichtet werden – die Konfiguration des Netzwerkzugangs und eines Webbrowsers genügt. Je nach Abrechnungsmodell kann damit auch eine Überlizenzierung der Unternehmenssoftware vermieden werden, da auf die Software nur bei tatsächlicher Benutzung zugegriffen wird und sich dies sehr leicht messen lässt (sog. nutzungsabhängige Abrechnung oder „pay as you go“).[93] Hier kommen zwei Modelle des Cloud-Computings in Betracht: Private und Public Cloud-Computing.[94] Natürlich können Unternehmen auf kommerzielle, jedem zugängliche Cloud-Computing-Angebote zugreifen (*Public Cloud-Computing*). Es besteht aber auch die Möglichkeit, eine unternehmensinterne, eigene (*Private*) Cloud-Computing-

[90] So etwa *Google Text&Tabellen*.

[91] Vgl. zu Chancen und Risiken der Auslagerung zentraler Unternehmensprozesse *Schulz*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 403, 408 ff.

[92] Vgl. eine Übersicht bei *Karger/Sarre*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 427, 428 f.

[93] *Schulz/Rosenkranz*, ITRB 2009, 232.

[94] Zur Abgrenzung im Einzelnen *Baun*, et al., Cloud Computing, 2010, S. 25 f.

Umgebung einzurichten und somit die Software und Daten aller Mitarbeiter im eigenen Netzwerk zentral verwalten zu können. Der Unterschied besteht hauptsächlich darin, auf wessen Server die jeweilige Anwendung ausgeführt wird und wer Zugriff auf die gemeinsam genutzten Ressourcen hat.[95] Private Cloud-Computing-Umgebungen können so eingerichtet werden, dass sie nur aus dem internen Firmennetzwerk zugänglich sind, was die Sicherheit der Anwendung vor externen Angriffen erheblich erhöht.

Im privaten Bereich kann Software als Cloud-Computing-Anwendung aufgrund der geringen individuellen Bereitstellungskosten meist kostenlos bzw. werbefinanziert oder für vergleichsweise geringe monatliche oder jährliche Pauschalbeträge angeboten werden. Im gleichen Maße, in dem die Kommerzialisierung des Internet fortschreitet und Methoden zur Abgeltung von Kleinbeträgen („micropayments“) etabliert werden, ist zu erwarten, dass diese Dienste zunehmend kostenpflichtig werden. Mit zunehmender Entwicklung des Funktionsumfangs wird von Cloud-Computing Angeboten als direkter Konkurrenz zu traditioneller Software reger Gebrauch gemacht.

### *3. Cloud-Computing in der öffentlichen Verwaltung*

In gewissen Konstellationen kann die Einrichtung von behördeninternen Private Cloud-Computing-Konfigurationen sinnvoll sein.[96] Für zentrale Verwaltungsaufgaben, etwa der Verwaltung von Bürgerdaten oder im Justizwesen, wird hierzulande (noch) keine kommerzielle, jedem zugängliche Public Cloud-Computing-Anwendungen eingesetzt.[97] In den U.S.A. hingegen setzen bereits einige Stadtverwaltungen aus Kosten- und Effizienzgründen auf die frei zugänglichen Cloud-Computing-Lösungen von Google.[98]

Da die Verwaltung in vielen Bereichen auf den Einsatz kommerziell verfügbarer Softwarelösungen angewiesen ist, spricht grundsätzlich nichts gegen den Einsatz von Cloud-Computing in der öffentlichen Verwaltung, solange Sicherheits- und Datenschutzbestimmungen eingehalten werden.[99] Die Technologien mögen derzeit noch in den Kinderschuhen stecken und werden deswegen teilweise zu Recht kritisiert.[100] Auf lange Sicht ist jedoch zu erwarten, dass die Verwaltung auch hierzulande dem Kostendruck und dem allgemeinen Trend der kommerziellen Anwendungssoftware folgen wird, was zunehmende Nutzung von Cloud-Computing-Lösungen mit einbezieht. Gera-

---

[95] *Armbrust*, et al., Above the Clouds: A Berkeley View of Cloud Computing, 2009, 3.

[96] *Schulz*, MMR 2010, 75, 76.

[97] *Schulz*, MMR 2010, 75, 76.

[98] So etwa die Stadtverwaltungen von Los Angeles und Washington D.C., vgl. *Schindler/Kalenda*, Stadtverwaltung Los Angeles nutzt künftig Google Apps, http://www.zdnet.de/news/wirtschaft_unternehmen_business_stadtverwaltung_los_angeles_nutzt_kuenftig_google_apps_story-39001020-41522080-1.htm (Stand: 26.01.2010).

[99] Zur Entwicklung des „E-Government“ und zu Aspekten der IT-Beschaffung in der Verwaltung: *Heckmann*, CR 2005, 711.

[100] *Schaffry*, CIOs in Behörden wollen keine IT in der „Wolke“, www.cio.de/882695 (Stand: 26.01.2010).

de aus Effizienz- und Kostengründen erscheint Cloud-Computing auch für die öffentliche Verwaltung als bedeutende Alternative zu derzeitigen Softwarelösungen.[101]

Aber auch umgekehrt ist es denkbar, dass der Staat eigene IT-Dienstleister hervorbringt, die – in den Grenzen der Zulässigkeit – auf dem Markt selbst als Anbieter von Cloud-Computing-Anwendungen auftreten.[102] Es bleibt abzuwarten, ob oder inwieweit daraus weitere Probleme entstehen, etwa bei den Grenzen staatlicher Ermittlungs- oder Eingriffsbefugnisse, wenn betroffene Daten bereits in der Hand einer Behörde sind.

### *II. Rechtliche Bewertung*

Das Phänomen Cloud-Computing berührt eine Vielzahl von Rechtsgebieten. Im Folgenden werden ausgewählte rechtliche Besonderheiten des Cloud-Computing im Zivilrecht, Urheberrecht, Straf- und Strafverfolgungsrecht, Datenschutzrecht sowie im öffentlichen Recht dargestellt, die für diese neue Erscheinungsform charakteristisch sind.[103]

#### *1. Zivilrecht*

Bei Cloud-Computing-Anwendungen bestehen Vertragsbeziehungen zwischen dem Nutzer und einem oder mehreren Cloud-Computing-Anbietern, die Leistungen wie die Bereitstellung von Online-Anwendungen und Online-Speicher erbringen.[104] Interne Vertragsverhältnisse im Anbieterbereich, beispielsweise die Installation der Cloud-Computing-Anwendung in nur virtuell existierenden, angemieteten Servern von Drittanbietern, bleiben hier außen vor.[105]

##### *a) Anwendbares Recht*

Bei Auslandsbezug stellt sich die Frage, welches Recht im Konfliktfall Anwendung findet. Dies hängt von der Ausgestaltung der tatsächlichen und vertraglichen Verhältnisse zwischen den Beteiligten im Einzelfall ab.[106]

---

[101] *Schulz*, MMR 2010, 75, 76.

[102] So etwa die *Anstalt für Kommunale Datenverarbeitung in Bayern* (www.akdb.de), vgl. *Heckmann*, CR 2005, 711, 715.

[103] Ein Überblick zu weiteren Problemkreisen, u.a. Compliance und IT-Sicherheit, bietet etwa *Niemann/Paul*, K&R 2009, 444.

[104] Vgl. *Söbbing*, MMR 2008, XII, XIII, der bei mehreren Leistungserbringern zwischen der Konstellation eines Generalunternehmers mit Subunternehmern und der des Vendor-Managements unterscheidet.

[105] Vgl. dazu etwa *Söbbing*, MMR 2008, XII, XIII; *Armbrust*, et al., Above the Clouds: A Berkeley View of Cloud Computing, 2009, S. 19.

[106] Zum deutschen Internationalen Privatrecht *Ullrich*/*Lejeune*, Der internationale Softwarevertrag, 2. Aufl. 2006, I Rn. 558 ff. Eine vertragliche Rechtswahl ist, auch gegenüber Verbrauchern, grundsätzlich möglich, *Schulz/Rosenkranz*, ITRB 2009, 232, 236.

Computersoftware gilt nach allgemeiner Ansicht als Ware im Sinne des *Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf* (CISG), wenn sie über einen Datenträger nutzbar und dadurch verkörpert ist, auch wenn sie über das Internet vertrieben wird.[107] Jedoch gilt das CISG nur, wenn die Ware dem Kunden vollständig überlassen wird und der Schwerpunkt nicht auf einer Gebrauchsüberlassung liegt,[108] wie es beim Cloud-Computing aber gerade der Fall ist. Insbesondere zeichnet sich Cloud-Computing vor allem im Business-to-Business-Bereich dadurch aus, dass die Software eine Eigenentwicklung des Dienstanbieters ist, die ausschließlich auf den Servern des Anbieters genutzt werden kann, also vom Anbieter gar nicht zum Kauf oder Lizenzerwerb zur Verwendung auf eigenen Rechnern angeboten wird. Das CISG gilt daher nicht für typische Verträge im Zusammenhang mit der Nutzung von Cloud-Computing-Angeboten.

Seit dem 17.12.2009 gilt nach Art. 3 EGBGB die Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I) unmittelbar. Betrifft der Vertrag einen Sachverhalt mit Auslandsbezug und ist keine Rechtswahl durch die Parteien getroffen (Art. 3 Rom-I-VO), bzw. ergibt sich kein anwendbares Recht aus Spezialgesetzen, so gelten die Art. 4 ff. Rom-I-VO zur Bestimmung des anwendbaren Rechts. Nach Art. 4 Abs. 1 b) bzw. Abs. 2 Rom-I-VO[109] gilt das Recht des Staates, in dem der Leistungserbringer seinen gewöhnlichen Aufenthalt hat. Für juristische Personen ist dies nach Art. 19 Abs. 1 Rom-I-VO der Ort der Hauptverwaltung. Ist der Anwender allerdings Verbraucher, gilt nach Art. 6 Rom-I-VO[110] das Recht des Staates, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat, jedoch unter der Bedingung, dass der Anbieter seine berufliche oder gewerbliche Tätigkeit auch in jenem Staat ausübt (Abs. 1 a)), oder eine solche Tätigkeit auf irgendeiner Weise auf diesen Staat ausrichtet (Abs. 1 b)). Aufgrund der sehr offenen Formulierung des Art. 6 Abs. 1 a) Rom-I-VO wird dies für alle in Deutschland abrufbare Onlineangebote regelmäßig zutreffen, also für Verbraucher stets deutsches Recht anwendbar sein. Dass bei Cloud-Computing der genaue Ort der Datenverarbeitung, also Ort der eigentlichen Leistungserbringung, oft nicht bekannt ist, spielt also für die Bestimmung des anwendbaren Rechts keine Rolle.

Gerade der Anbieter muss sich bewusst sein, dass er sich durch das weltweite – auch unentgeltliche – Anbieten seiner Leistung möglicherweise einer Vielzahl internationaler und unüberschaubarer Vertragsbeziehungen aussetzt. Dies kann weitreichende Konsequenzen haben, etwa ist ein Haftungsausschluss nach den dann anwendbaren deutschen

[107] BeckOK CISG/*Saenger*, 15. Aufl. 2009, Art. 1 Rn. 7.
[108] BeckOK CISG/*Saenger*, 15. Aufl. 2009, Art 1 Rn. 3.
[109] Bis zum 16.12.2009 galt entsprechend § 28 Abs. 1 S. 1 EGBGB a.F.
[110] Vgl. § 29 Abs. 2 EGBGB a.F.

Regeln zu allgemeinen Geschäftsbedingungen nicht pauschal möglich (vgl. § 309 Nr. 7 BGB).[111]

### *b) Vertragstypologie*

Neben der Frage nach dem anwendbaren Recht stellen sich auch Probleme bei der Bestimmung der Vertragstypologie. Für das deutsche Recht hat die genaue Festlegung nicht nur Konsequenzen im Hinblick auf das jeweils anwendbare Mängelrecht, sondern auch auf die Auslegung der Vertragspflichten und Leitbilder der AGB-Kontrolle.[112] Die Bereitstellung von Cloud-Computing-Angeboten unterscheidet sich von herkömmlichen Softwarelieferungsverträgen dadurch, dass nicht an einen physikalischen Datenträger als Gegenstand eines Kaufvertrages angeknüpft werden kann.[113] Da der serverseitige Teil der Software stets beim Anbieter verbleiben soll und ohne dessen Bereitstellung nicht oder nur sehr eingeschränkt nutzbar ist, ist die Anwendung von Kaufrecht nach der Natur der Sache ausgeschlossen.

Hingegen wird für die meisten Fälle des Cloud-Computing, wie schon bei Softwareoutsourcing und ASP[114], ein typengemischter Vertrag[115] mit im Wesentlichen miet- bzw. leihvertraglichem Charakter anzunehmen sein (§ 535 bzw. § 598 BGB),[116] da dem Anwender über das Internet vermittelt Hard- und Softwareleistungen gegen Entgelt oder kostenlos für die Dauer der Nutzung zur Verfügung gestellt werden. Eine Besitzverschaffung am Miet- bzw. Leihgegenstand ist nicht Voraussetzung für diese Vertragstypen, sofern die vertragliche Gebrauchsüberlassung auch ohne Besitz erreicht wird.[117] Schon 1993 hat der BGH im Zusammenhang mit der stundenweisen Überlassung eines Großrechners entschieden, dass Rechenzeit tauglicher Gegenstand von Mietverträgen sein kann.[118] Zu dieser Zeit haben die wenigen verfügbaren Hochleistungsrechenzentren

---

[111] *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, Rn. 601 f.; *Ullrich*/*Lejeune*, Der internationale Softwarevertrag, 2. Aufl. 2006, I Rn. 505 ff.

[112] *Schulz*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 403, 406.

[113] Hier kommt es im Einzelfall auf den genauen Vertragsgegenstand an. Vgl. *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, S. 96; *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, Rn. 674 ff. Teilweise wird Software als Kauf von Rechten oder sonstigen Gegenständen im Sinne des § 453 BGB eingeordnet, vgl. *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, Rn. 674.

[114] Für ASP ausdrücklich *BGH*, Urteil vom 15.11.2006 - XII ZR 120/04, MMR 2007, 243; *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, Rn. 729 ff.; *Söbbing*, MMR 2008, XII, XIV unterscheidet zwischen Applikationsnutzung und Datenbankhosting.

[115] *Niemann/Paul*, K&R 2009, 444; *Schulz/Rosenkranz*, ITRB 2009, 232, 233; vgl. *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, Rn. 451 ff.

[116] *Pohle/Ammann*, CR 2009, 273, 275; vgl. zu den daraus folgenden Problemen *Karger/Sarre*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 427, 432 f.

[117] *Schneider*, Handbuch des EDV-Rechts, 4. Aufl. 2009, C Rn. 208; die eigentliche Leistung kann auch nur die Verfügbarkeit der Rechenleistung sein, vgl. Müko-BGB/*Häublein*, 2006, § 535 Rn. 67; *Gennen*/*Völkel*, Recht der IT-Verträge, 2009, Rn. 743.

[118] *BGH*, NJW-RR 1993, 178.

ihre Rechenkapazitäten für Externe zur Verfügung gestellt und nach Zeit abgerechnet.[119] Der Anwender konnte über eine Schnittstelle, etwa ein Computernetzwerk, Informationen eingeben, die der Hochleistungsrechner intern verarbeitet und das Verarbeitungsergebnis ausgegeben hat. Dies unterscheidet sich im Wesentlichen nicht von modernen IT-Lösungen, die lediglich grafisch und technisch aufwendigere Eingabemasken vorsehen und einer breiteren Masse zugänglich sind. Auf der technischen Ebene werden auch hier Informationen über eine Schnittstelle zur Verarbeitung an ein Rechenzentrum weitergeben. Der BGH hat 2006 seine Überlegungen daher richtigerweise auch auf Verträge zu modernem Application Service Providing übertragen und die Nutzungsverträge als mietvertraglich eingeordnet.[120] Für die nächste Stufe, das Cloud-Computing, kann nichts anderes gelten.

Letztlich unterscheidet sich Cloud-Computing von reiner Rechenzeitmiete[121] im Wesentlichen durch die einfachere Handhabe und weitere Verbreitung sowie die umfassenderen Programmfunktionen in der Benutzerschnittstelle, die sich nicht mehr nur auf reine Rechenleistung beschränken. Nach wie vor greift der Anwender über Schnittstellen auf Datenträger in Rechenzentren zu, auf denen Software verkörpert ist und auch verbleibt; die eigentliche Leistung ist die Verfügbarkeit.[122] Wie aufwändig die Benutzerschnittstelle gestaltet ist sowie die Tatsache, dass der tatsächliche Ausführungs- und Speicherungsort der Software aufgrund der weltweiten Vernetzung der Serverfarmen möglicherweise nicht präzise bestimmt werden kann, ändern nichts an der für Miet- bzw. Leihverträgen charakteristischen Grundsituation: Dem Benutzer wird die Serverhardware und die im Regelfall proprietäre Software des Anbieters (gegen Entgelt) auf Zeit zur Verfügung gestellt.[123]

### *2. Urheberrecht*

Urheberrechtliche Aspekte lassen sich beim Cloud-Computing sowohl aus Sicht des Anbieters als auch aus Sicht des Kunden betrachten. Der Anbieter hat als Urheber der auf dem Server ausgeführten Computerprogramme grundsätzlich alle Rechte an seiner Software (§§ 69, 69c UrhG).[124] Sofern die konkrete Ausgestaltung der Anwendung es erfordert, dass der Benutzer einzelne Programmelemente auf seinen Arbeitsspeicher herunterlädt und ggf. in den Zwischenspeicher auf seiner Festplatte kopiert, ist dies eine Vervielfältigungshandlung an Teilen der Software, nicht jedoch an der Anwendungs-

[119] *Schneider*, Handbuch des EDV-Rechts, 4. Aufl. 2009, M Rn. 1.
[120] *BGH*, Urteil vom 15.11.2006 - XII ZR 120/04, MMR 2007, 243.
[121] Ein Phänomen vor allem bei Großrechenanlagen in den 60er und 70er-Jahren.
[122] *Schneider*, Handbuch des EDV-Rechts, 4. Aufl. 2009, C Rn. 208.
[123] Vgl. *BGH*, NJW-RR 1993, 178; *BGH,* MDR 2007, 257.
[124] Zur Anwendbarkeit in Deutschland Bröcke/Czychowsk/Schäfer/*Nordemann-Schiffel*, Praxishandbuch geistiges Eigentum im Internet, 2003, § 3 Rn. 36 ff.; *Hoeren*, Internet- und Kommunikationsrecht, 2008, Rn. 110 ff.

software selbst.[125] Die einzelnen Softwareelemente werden dem Benutzer zur Verfügung gestellt, also etwa das Programminterface, klickbare Buttons oder Icons. Der Anbieter räumt dem Benutzer insofern – wenn die Einzelelemente überhaupt die hinreichende Schöpfungshöhe nach § 2 Abs. 2 UrhG erreichen[126] – ein entsprechendes Nutzungsrecht ein.[127] Unabhängig von der Frage, ob § 44a UrhG auch auf Cloud-Computing-Programme Anwendung findet,[128] liegt durch das öffentliche Anbieten jedenfalls eine Zustimmung zu diesen Vervielfältigungshandlungen vor.

Die ordnungsgemäße Benutzung von Cloud-Computing-Anwendungen setzt zwingend die Mitwirkung seitens des Serverbetreibers voraus. Anders als traditionelle Software lassen sich die Anwendungen nicht auf den heimischen PC laden und dort „offline" ausführen. Charakteristisches Merkmal von Cloud-Computing-Anwendungen ist ihre Benutzbarkeit nur im Zusammenhang mit einer Netzwerkkommunikation, etwa einer bestehenden Internetverbindung. Eine bestimmungsgemäße Benutzung der Anwendung ohne Wissen des Anbieters kommt bereits technisch bedingt nicht in Betracht. Da der berechtigten Nutzung der Anwendung stets ein entsprechender Vertrag zugrunde liegen wird und die Anwendung nach dem Konzept des Cloud-Computings nur auf den Servern des Anbieters lauffähig ist, bleibt kaum ein Anwendungsbereich für § 69d UrhG zur Rechtfertigung von Vervielfältigungshandlungen an der Software.[129]

### *3. Strafrecht*

Im Folgenden werden einige Besonderheiten des Cloud-Computings aus strafrechtlicher Sicht betrachtet.

#### *a) Arten möglicher Delikte*

Grundsätzlich lassen sich alle Straftaten mit Bezug zum Internet auch im Zusammenhang mit Cloud-Computing begehen. Die Funktion, bearbeitete Dateien auf den Servern abzuspeichern oder zwischen mehreren Bearbeitern zu teilen, ermöglicht beispielsweise sämtliche Datenveränderungs-, Äußerungs- und Verbreitungsdelikte. Der Benutzer kann gegenüber dem Anbieter Computerbetrugsdelikte begehen, etwa die Verwendung unrichtiger oder unvollständiger Daten bei Vertragsabschluss (§ 263a Abs. 1 Var. 2 StGB). Er kann, entsprechende Sachkenntnis vorausgesetzt, unbefugt in den Ablauf der Programme und Serverfunktionen einwirken (§ 263a Abs. 1 Var. 4 StGB), Daten verän-

[125] Dreier/Schulze/*Dreier*, UrhG, 3. Aufl. 2008, § 69d, Rn. 8; *Schuster/Reichl*, CR 2010, 38, 40; *Niemann/Paul*, K&R 2009, 444, 448.

[126] Dreier/Schulze/*Dreier*, UrhG, 3. Aufl. 2008, § 69a, Rn. 16; den Schutz darüber hinaus auch auf den zugrunde liegenden Befehlssatz ausweitend *Alpert*, CR 2003, 718, 719.

[127] *Niemann/Paul*, K&R 2009, 444, 448.

[128] Anwendung auf Software generell umstritten, vgl. Dreier/Schulze/*Dreier*, UrhG, 3. Aufl. 2008, § 44a Rn. 2.

[129] Anders argumentieren *Pohle/Ammann*, CR 2009, 273.

dern (§ 303a StGB) oder die Datenverarbeitung stören (§ 303b StGB). Täter können auch auf die Datenverarbeitung Dritter Einfluss nehmen: Speichert ein Unternehmen etwa Geschäftsvorfälle in einer Cloud-Computing-Anwendung, könnte ein Hacker diese ausspähen (§ 202a StGB) oder sie verändern, z.B. seine Bestellung als bezahlt markieren (vgl. § 270 StGB).

Neben Angriffen auf die Cloud-Computing-Struktur ist aber auch möglich, Straftaten unter Verwendung von Cloud-Computing-Anwendungen zu begehen. Zu denken ist etwa an das massenhafte Versenden von Spam-Nachrichten über die Server des Anbieters oder ein sog. (Distributed) Denial of Service-Angriff (DDoS)[130], bei dem die Funktionsweise eines Servers durch massenhafte Anfragen beeinträchtigt wird. Die kurzfristige Verfügbarkeit enormer Rechenleistungen erlaubt es auch, rechenintensive Angriffe auf Verschlüsselungssystem durchzuführen (z.B. Brute-Force-Attacken[131]).

*b) Anwendbarkeit deutschen Strafrechts*

Ländergrenzen verlieren im Internet zunehmend an Bedeutung. Hat eine Tat grenzüberschreitenden Bezug ist zunächst festzustellen, ob deutsches Strafrecht anwendbar ist. Hier gelten grundsätzlich die gleichen Regeln wie bei allen Taten im Zusammenhang mit dem Internet.[132] Die Strafanwendungsregeln des Strafgesetzbuches (§§ 3–9 StGB) sind insbesondere aufgrund des Ubiquitätsprinzips (§ 9 StGB) sehr weitreichend. Jede Handlung und jeder Erfolg in Deutschland führt zur Anwendbarkeit deutschen Strafrechts (Ubiquitätsprinzip).[133] Bedient der Täter die Cloud-Computing-Anwendung aus Deutschland heraus oder richtet sich die Tat gegen ein Datenverarbeitungssystem in Deutschland, ist die Anwendbarkeit deutschen Strafrechts grundsätzlich gegeben.[134]

Bei Gefährdungsdelikten kann der Erfolg allerdings auch in der über das Internet vermittelte Verursachung einer konkreten Gefahr im Inland gesehen werden.[135] Gibt etwa jemand bei *Google Text&Tabellen* eine Seite mit illegalem Inhalt frei, sodass jeder darauf zugreifen kann, entspricht dies im Wesentlichen der Erstellung einer eigenen Webseite. Schon durch diese Veröffentlichung kann nach der Argumentation der Recht-

[130] Vgl. **Es ist eine ungültige Quelle angegeben.**.

[131] Zu dieser und weiterer Angriffsformen *Lassmann*, Wirtschaftsinformatik, 2006, S. 358 ff.

[132] Vgl. *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 78 ff.

[133] Vgl. *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 220 ff.; *Marbeth-Kubicki*, Computer- und Internetstrafrecht, 2005, S. 21 ff.; *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 75 ff.

[134] Vgl. ausführlich zum Problemkomplex hinsichtlich Cloud-Computing aus amerikanischer Sicht *Christos Velasco San Martin*, Jurisdictional Aspects of Cloud Computing, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf (Stand: 12.3.2010)

[135] Vgl. *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 226.

sprechung unabhängig vom Serverstandort eine Gefährdung im Inland eintreten, somit einen Erfolgsort begründen was deutsches Strafrecht zur Anwendung bringt.[136]

Ein besonderer Fall tritt auch ein, wenn der im Ausland ansässige Täter deutsche Cloud-Computing-Server einsetzt, die Tat (etwa ein Denial-of-Service-Angriff[137]) sich aber wiederum nur gegen Rechtsgüter im Ausland richtet. Es stellt sich die Frage, ob dies allein zur Anwendbarkeit deutschen Strafrechts führen kann, also ob der Handlungs- oder Erfolgsort nach § 9 Abs. 1 StGB in diesem Fall in Deutschland liegt.

Unter Handlungsort wird jeder Ort verstanden, an dem der Täter eine auf die Tatbestandsverwirklichung gerichtete Tätigkeit vornimmt, also der Ort des körperlichen Tätigwerdens,[138] hier also nicht Deutschland. Teilweise wird dagegen argumentiert, der Handlungsort wäre bei Fernsteuerung eines Rechners über das Internet gleichzeitig am Ort der unmittelbaren Dateneingabe und am Serverstandort, da eingegebene Daten über die Netzwerkstruktur unmittelbar auch auf der Empfangsseite wirken.[139] Der Handlungsort würde also räumlich auseinanderfallen, vergleichbar zu mehraktigen Delikten mit Einzelhandlungen an verschiedenen Orten.[140] Kritiker argumentieren, dass nicht scharf genug zwischen Handlung (dem körperlichen Eingeben von Daten) und der Wirkung der Handlung (die Verarbeitung auf dem Server) unterschieden wird.[141] Der Verarbeitung am Server kommt keine eigene Handlungsqualität zu, Handlungsort ist in solchen Fällen nur der Ort, an dem der Täter unmittelbar Daten eingibt.[142] Da also hier sowohl Tathandlung als auch Taterfolg im Ausland liegen, handelt es sich um ein sog. Transitdelikt[143], welches nicht die Anwendbarkeit deutschen Strafrechts nach § 9 StGB begründet. Sind nicht noch andere Delikte erfüllt, etwa der Besitz von „Hackertools“ (§ 202c Abs. 1 Nr. 2 StGB),[144] bleibt es beim Grundgedanken des § 9 StGB, wonach nur bei tatsächlicher Schädigung oder Gefährdung von Rechtsgütern im Inland deutsches Strafrecht zur Anwendung kommen soll.[145]

---

[136] So der *BGH* zur Verbreitung der „Auschwitzlüge“ im Internet, MMR 2001, 228.

[137] Dazu *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 197; BeckOK-StGB/*Weidemann*, 10. Aufl. 2009, § 303b Rn. 10; nach der Gesetzesbegründung soll dies von § 303b StGB erfasst sein, vgl. BT-Drs. 16/3656, 13.

[138] BeckOK-StGB/*Heinegg*, 10. Aufl. 2009, § 9 Rn. 2; vgl. *BGH*, NStZ 2007, 287; *Cornils*, JZ 1999, 394, 396 f.

[139] So etwa *Cornils*, JZ 1999, 394, 395 f.; vgl. Schönke/Schröder/*Eser*, StGB, 27. Aufl. 2006, § 9 Rn. 4.

[140] *Cornils*, JZ 1999, 394, 396 f.

[141] *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 241; *Gercke*, Rechtswidrige Inhalte im Internet, 2000, S. 20 f.; *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 80.

[142] *Gercke*, Rechtswidrige Inhalte im Internet, 2000, S. 21.

[143] BeckOK CISG/*von Heintschel-Heinegg*, 15. Aufl. 2009, Lexikon des Strafrechts, Rn. 41

[144] Vgl. *Cornelius*, CR 2007, 682; Leupold/Glossner/*Cornelius*, MAH IT-Recht, 1. Aufl. 2008, Teil 8, Rn. 82 ff.; *Valerius*, JR 2010, 84 ff.

[145] MüKo-StGB/*Ambos/Ruegenberg*, 2003, § 9 Rn. 23; vgl. bzgl. einer möglichen teleologischen Reduktion des § 9 StGB *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 242 ff.

*c) Ausspähen von Daten (§ 202a StGB) im Zusammenhang mit Cloud-Computing*

Insbesondere das Ausspähen von Daten (§ 202a StGB) ist im Zusammenhang mit Online-Datenverarbeitung von besonderer Relevanz. Durch die Verlagerung großer Datenbestände oder besonders sensibler Daten auf weltweit zugängliche Webserver werden sie einer besonderen Gefährdung ausgesetzt.[146] Muss sich bei rein lokaler Datenverarbeitung ein Täter physikalischen Zugang zu Speichermedien verschaffen, reicht bei Onlineanwendungen meist die Eingabe des richtigen Passwortes, um Zugriff auf sämtliche Daten zu erhalten. Da die Daten weder selbst Geheimnis, noch von irgendeinem Wert als Teil des Vermögens des Opfers sein müssen,[147] sind dabei grundsätzlich alle im Cloud-Computing abgelegten Daten[148] taugliche Tatobjekte des § 202a StGB. Vom Tatbestand werden sowohl gespeicherte als auch übermittelte Daten erfasst.

Träger des Rechtsgutes ist der über die Daten Verfügungsberechtigte, was sich nach dem Akt der Erschaffung richtet, nicht jedoch nach dem Eigentum am Datenträger oder danach, wen die Daten inhaltlich betreffen.[149] Beispielhaft für die Begründung der Verfügungsmacht werden der Skripturakt und der erstmalige Speicherungsvorgang genannt.[150] Beim Cloud-Computing kommen sowohl der Anwender als auch der Anbieter als Verfügungsberechtigte in Betracht.[151] Letztlich teilt sich die Verfügungsmacht zwischen Anwender und Anbieter auf. Der Anwender hat als Veranlasser der Speicherung die Verfügungsmacht über die von ihm bearbeiteten Dateien, der Anbieter wiederum über die Datenbank bzw. die Datenarchive, in denen seine Kundendaten abgespeichert sind.[152]

Tathandlung des § 202a StGB, das sich Verschaffen von Daten, liegt vor, wenn der Täter durch optische und akustische Wahrnehmung von den Daten Kenntnis nimmt bzw. einem anderen dies ermöglicht, oder ohne Kenntnisnahme einen Datenträger in seine Verfügungsgewalt bringt bzw. auf einem eigenem Datenträger abspeichert.[153] Erfüllt ist der Tatbestand regelmäßig, wenn ein Täter einen physischen oder virtuellen

[146] In der Polizeilichen Kriminalstatistik (PKS 2009) wurde hinsichtlich Ausspähen von Daten ein Anstieg von 48,7 % auf 11.491 Straftaten allein vom Jahre 2008 auf 2009 registriert, PKS 2009 (http://www.bka.de/pks/pks2009/download/pks2009_imk_kurzbericht.pdf; 11.05.2010).

[147] *Marbeth-Kubicki*, Computer- und Internetstrafrecht, 2005, Rn. 54.

[148] Zum Datenbegriff *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 655; MüKo-StGB/*Graf*, 2003, § 202a Rn. 8 f.; Schönke/Schröder/*Lenckner*, StGB, 27. Aufl. 2006, § 202a Rn. 3.

[149] BeckOK-StGB/*Weidemann*, 10. Aufl. 2009, § 202a Rn. 7 ff.

[150] *Marbeth-Kubicki*, Computer- und Internetstrafrecht, 2005, Rn. 55, m.w.N.

[151] Die Verfügungsbefugnis richtet sich nach den jeweiligen Vereinbarungen. Zu den Kriterien *Hilgendorf*, Anm. zu BayObLG Entscheidung vom 24.06.1993, JR 1994, 476, 478 f.; MüKo-StGB/*Graf*, 2003, § 202a Rn. 17.

[152] Vgl. MüKo-StGB/*Graf*, 2003, § 202a Rn. 43 ff.; Schönke/Schröder/*Lenckner*, StGB, 27. Aufl. 2006, § 202a Rn. 10.

[153] *Marbeth-Kubicki*, Computer- und Internetstrafrecht, 2005, Rn. 57.

Server des Anbieters in seinen Besitz bringt. Probleme können sich an dieser Stelle ergeben, wenn der Anbieter die Daten nur verschlüsselt abspeichert oder nur einzelne Dateifragmente auf einem physikalischen Server gespeichert werden, wodurch die erlangten Daten faktisch wertlos sind.[154]

Voraussetzung des § 202a StGB ist, dass die Daten besonders gegen fremden Zugriff gesichert sind. Dies bedeutet, dass Vorkehrungen getroffen werden müssen, die den Zugriff Dritter zumindest nicht unerheblich erschweren, wodurch der Berechtigte sein Interesse an einer Geheimhaltung erkennbar zum Ausdruck bringt.[155] Die Daten der Benutzer sind üblicherweise nur nach Eingabe eines Passwortes zugänglich und insofern gegen unberechtigten Zugang besonders gesichert.[156]

Ein Sonderfall stellt die Möglichkeit vieler Cloud-Computing-Anwendungen dar, Dateien oder Dokumente unter Verwendung einer besonders kompliziert gestalteten, aber ohne weitere Passwortabfrage zugänglichen Webadresse freizugeben.[157] Der Schutz der Daten besteht hier lediglich in einer schwer zu erratenden Webadresse, die der Anwender an Dritte weitergeben kann. Allerdings kann jeder, der die genaue Adresse errät, ausspäht oder sich sonst verschafft, ebenso ungehindert auf alle Daten zugreifen. Üblicherweise wird das Tatbestandsmerkmal der besonderen Zugangssicherung dahingehend ausgelegt, dass Vorkehrungen getroffen werden müssen, die den Zugriff auf Daten ausschließen oder wenigstens nicht unerheblich erschweren und der Berechtigte sein Interesse an der Geheimhaltung erkennbar zum Ausdruck bringt.[158] Die Verwendung einer schwer zu erratenden Webadresse erfüllt diese Merkmale, zumal es keinen großen Unterschied macht, ob der Anwender eine geheime Zeichenfolge als Zugangsschlüssel in ein Passwortfeld oder als Teil der Webadresse eingeben muss. Durch die Geheimhaltung der genauen Adresse, die auch nicht in Suchmaschinen indiziert wird, macht der Anwender seinen Willen zur generellen Geheimhaltung deutlich.[159]

---

[154] Ein Verschaffen liegt dann nur vor, wenn eine Entschlüsselung technisch möglich ist, *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 684. Andere verlangen eine tatsächliche Entschlüsselung oder zumindest Besitz des Schlüssels, Schönke/Schröder/*Lenckner*, StGB, 27. Aufl. 2006, § 202a Rn. 10.

[155] Schönke/Schröder/*Lenckner*, StGB, 27. Aufl. 2006, § 202a Rn. 7.

[156] Auf eine besondere Wirksamkeit, etwa ein besonders sicheres Passwort, kommt es hierbei nicht an, vgl. Schönke/Schröder/*Lenckner*, StGB, 27. Aufl. 2006, § 202a Rn. 7 f.

[157] Bei *Google Text&Tabellen* können so etwa Dokumente freigegeben werden. Der Benutzer kann diese „geheime" Web-Adresse daraufhin an Mitarbeiter verteilen, die ohne Anmeldung auf die Daten zugreifen und auch verändern können.

[158] *Lackner*/*Kühl*, 26. Aufl. 2007, § 202a Rn. 4; BeckOK-StGB/*Weidemann*, 10. Aufl. 2009, § 202a Rn. 13; vgl. BT-Drs 10/5058, 29; BT-Drs 16/3656.

[159] Zum „Verstecken von Daten" als Zugangssicherung *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 662; MüKo-StGB/*Graf*, 2003, § 202a Rn. 41.

### *4. Herausforderungen für Strafverfolgungsbehörden*

Der traditionelle Ansatz der Strafverfolgungsbehörden bei Computerdelikten ist die Durchsuchung von Wohn- oder Geschäftsräumen und die Beschlagnahme von Computerhardware und Datenträgern.[160] Dieses Instrument verliert erheblich an Wirksamkeit, wenn relevante Daten über Cloud-Computing ins Internet ausgelagert werden. Sind für die Strafverfolgung bedeutsame Daten nicht mehr lokal gespeichert,[161] sondern nur auf den Servern der Anbieter, muss ein anderer Ansatz zur Beweissicherung gewählt werden. Hierbei sind drei Problembereiche zu betrachten:

#### *a) Speicherort der Daten*

Der erste Problembereich betrifft das Auffinden des genauen Speicherorts der Daten. Setzt der Cloud-Computing-Anbieter etwa Technologien zur Virtualisierung und dynamischen Ressourcenoptimierung ein, wird der Speicherort einer Datei vom System ohne Einflussmöglichkeit des Betroffenen entsprechend der Ressourcenverfügbarkeit bestimmt. Zusätzlich können Dateien fragmentiert, d.h. bruchstückhaft über mehrere Speicherorte verteilt, gespeichert werden.[162] Dies geschieht für den Benutzer völlig transparent, selbst der Anbieter ist unter Umständen nicht in der Lage, den genauen Speicherort einer Datei zu ermitteln.[163] Einige Anbieter bieten auch an, alle Daten so verschlüsselt abzuspeichern, dass nur der Benutzer selbst auf diese zugreifen kann.[164] Ein Zugriff auf die Daten ist also unter Umständen nur über die Anwenderoberfläche der jeweiligen Anwendung unter Verwendung des Benutzerpasswortes möglich. Für die Strafverfolgungsbehörden kann dies bedeuten, dass ein Zugriff auf die Daten gänzlich ausgeschlossen ist oder der genaue Speicherort jeder Datei bzw. jedes Dateifragments unter erheblichem Aufwand gesondert ermittelt werden muss.

#### *b) Internationalität der Speicherverteilung*

Der zweite Problembereich liegt in der Internationalität von Cloud-Computing-Infrastrukturen. Wie bereits dargestellt betreiben viele Anbieter ihre Servernetzwerke weltweit. Zwar wurde in § 110 Abs. 3 StPO eine grundsätzliche Befugnis geschaffen, Daten des Betroffenen auch auf räumlich getrennten Speichermedien einer Durchsicht zu unterziehen und sie ggf. zu sichern.[165] Befinden sich die Daten allerdings auf einem

---

[160] Vgl. *Obenhaus*, NJW 2010, 651.

[161] In Betracht kommt etwa die computerforensische Untersuchung des lokalen Zwischenspeichers oder Caches, in welchem etwa zuletzt bearbeitete Dateien gespeichert sein könnten, *Geschonneck*, Computer-Forensik, 3. Aufl. 2008, S. 78, 86; *Willer/Hoppen*, CR 2007, 610, 614.

[162] *Baun*, et al., Cloud Computing, 2010, S. 13 ff.

[163] *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 976.

[164] So etwa Mozy, ein Dienst zur Online-Datensicherung, http://support.mozy.com/docs/en-user-home-win/guide/tasks/install_change_encryption_win_c.html (24.05.2010).

[165] Die genaue Rechtsgrundlage für eine Sicherstellung ist im Einzelfall zu ermitteln. Insbesondere hin-

ausländischen Speichermedium, ist Völkerrecht betroffen.[166] Aufgrund der völkerrechtlichen Souveränität der ausländischen Staaten haben deutsche Behörden keine unmittelbare Zugriffsmöglichkeit auf dort abgelegte Daten,[167] § 110 Abs. 3 StPO ist in seinem Anwendungsbereich auf Daten im Inland beschränkt. Zur Sicherung der Daten ist also stets die Zustimmung des fremden Staates oder des Berechtigten notwendig.[168]

Zudem wird bereits die direkte Anfrage eines deutschen Ermittlungsbeamten bei einem Anbieter im Ausland, ebenso wie ein staatlicher Zugriff auf Daten in der Cloud mit Hilfe eines über § 113 TKG erlangten Passwortes,[169] bereits als hoheitliche Maßnahme gegenüber diesem und somit als Verletzung des völkerrechtlichen Souveränitätsprinzips des anderen Landes angesehen.[170] Die Einhaltung der Verfahrensregeln zur internationalen Zusammenarbeit hat somit erhebliche Bedeutung und kann unter Umständen auch zu einem Verwertungsverbot führen.[171] Die Strafverfolgungsbehörden sind in diesem Bereich auf eine enge Kooperation mit den jeweiligen Behörden des betreffenden Landes angewiesen.[172]

Möglich bleibt ein Rückgriff etwa auf das Abhören der Kommunikation des Betroffenen mit dem Anbieter nach § 100a StPO, um so an entsprechende Daten zu gelangen.[173]

### *c) Möglicher Eingriff in den höchstpersönlichen Lebensbereich*

Ein Vorteil beim Einsatz von Cloud-Computing-Anwendungen gegenüber herkömmlicher Software ist die schnelle Verfügbarkeit und Durchsuchbarkeit aller Dateien über den Webbrowser, ohne dass die Daten auf den lokalen Arbeitsplatz geladen oder dort gespeichert sein müssen. Nutzt eine Person Cloud-Anwendungen etwa zur Textverar-

---

sichtlich E-Mails in Online-Postfächern bestehen dabei erhebliche Unklarheiten. So soll es sich um eine Postbeschlagnahme nach §§ 99, 95 Abs. 2 StPO handeln (*BGH*, NStZ 2009, 397), nach anderer Ansicht dagegen um eine Telekommunikationsüberwachung, wonach §§ 100a, 100b StPO als Eingriffsgrundlage in Betracht kommt (*LG Hamburg*, K&R 2008, 122); zur Verfassungsmäßigkeit *BVerfG*, MMR 2009, 673; ausführlich auch *Brodowski*, JR 2009, 402; zur Beschlagnahme von EDV-Daten *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rn. 404 ff.

[166] *Gercke*, ZUM 2009, 526, 536; *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 40; *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rn. 372 ff.

[167] *Sankol*, K&R 2008, 279.

[168] BeckOK-StPO/*Hegmann*, 5. Aufl. 2010, § 110 Rn. 4; vgl. zu dieser Einschränkung auch den ausdrücklichen Wortlaut des Art. 19 Abs. 2 der Cybercrime Konvention des Europarates. Zudem ist durch den unautorisierten Abruf eine Eigentumsverletzung des jeweiligen Anbieters nach dessen Rechtsordnung denkbar.

[169] *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 657.

[170] *Gercke*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 499, 503.

[171] *Gercke*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 499, 502; vgl. BeckOK-StPO/*Volk*, 5. Aufl. 2010, § 100a Rn. 14, 133.

[172] *Gercke*, CR 2004, 784, 785.

[173] Dies kommt aufgrund des Katalogs in § 100a Abs. 2 StPO nur im Bereich der Schwerkriminalität in Betracht.

beitung und Dateiverwaltung, so entspricht eine Durchsuchung der Dateien auf dem Server letztlich einer Durchsuchung von lokalen Dateien, wenn herkömmliche Software eingesetzt worden wäre. Eine Behörde könnte daher etwa – entsprechende Eingriffsnormen und Zugangsmöglichkeiten vorausgesetzt – in Sekundenbruchteile alle Textverarbeitungsdokumente eines Betroffenen nach Schlüsselbegriffen durchsuchen, ohne dessen Räume betreten zu müssen. Besonders problematisch wird dies soweit Cloud-Computing-Angebote auch zur Speicherung von Daten genutzt werden, die den höchstpersönlichen Lebensbereich betreffen.

Das Bundesverfassungsgericht hat zur „Onlinedurchsuchung“ in seiner neueren Rechtsprechung ein neues „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ geschaffen.[174] Dieses soll einschlägig sein, wenn der Zugriff auf das betreffende informationstechnische System Dritten ermöglicht, „einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten”.[175] Auch in Cloud-Anwendungen können persönliche Daten gespeichert werden, „die dem Kernbereich zuzuordnen sind. So kann der Betroffene das System dazu nutzen, Dateien höchstpersönlichen Inhalts, etwa tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente, anzulegen und zu speichern.“[176] Die Argumentation des Bundesverfassungsgerichts, wonach bei heimlichen Überwachungsmaßnahmen ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren ist und dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt, [177] lässt sich daher unmittelbar auch auf Cloud-Computing-Angebote übertragen.

Dieses Grundrecht muss folglich auch bei anderen Eingriffsbefugnissen berücksichtigt und bei der Abwägung der Verhältnismäßigkeit mit einbezogen werden. So sieht etwa § 20k BKAG, der den verdeckten Eingriff in informationstechnische Systeme erlaubt, in Abs. 7 ausdrücklich ein Verwertungsverbot und eine Löschungspflicht für solche höchstpersönlichen Daten vor.[178]

### *5. Datenschutzrecht*

Cloud-Computing eignet sich unter anderem auch für Verwaltung großer Datenbestände. So können etwa Datenbanken mit Kundendaten online verwaltet werden, die auch personenbezogene Daten nach § 3 BDSG beinhalten können. Eine Grundkonzeption des Cloud-Computings ist es, dass die Daten für den Nutzer transparent auf den Ser-

[174] *BVerfG*, NJW 2008, 822.

[175] *BVerfG*, NJW 2008, 822, 827 Rn. 203.

[176] *BVerfG*, NJW 2008, 822, 833 Rn. 272.

[177] *BVerfG*, NJW 2008, 822, 833 Rn. 272; vgl. *BVerfG,* NJW 1957, 297; *BVerfG*, NJW 1973, 891; *BVerfG,* NJW 2004, 999; *Kutscha*, NJW 2008, 1042.

[178] Vgl. *Roggan*, NJW 2009, 257, 259 ff.; das *BVerfG* hat dazu ein „zweistufiges Schutzkonzept“ entwickelt, NJW 2008, 822, 834 Rn. 280 ff.

vern der Anbieter gespeichert werden. Entsprechend der Verteilung der IT-Ressourcen sind diese Daten bei international operierenden Anbietern regelmäßig in weltweit verteilten, untereinander vernetzten Datenbanken gespeichert. Die einzelnen Datenströme werden ressourcenoptimiert automatisch im gesamten Servernetz verteilt. Zudem wird der Anbieter regelmäßige Sicherungskopien aller Datenbestände anlegen, die er aus Sicherheitsgründen örtlich getrennt speichern wird. Je nach Größe und weltweiter Verbreitung der Serverstandorte ist es sowohl für den Nutzer als auch für den Betreiber unmöglich, den genauen Speicherort der sie betreffenden Daten zu bestimmen. Teilweise ist sogar die nachträgliche Ermittlung des genauen Speicherortes nicht mehr möglich.

Werden personenbezogene Daten im Inland erhoben, verarbeitet oder genutzt, gilt grundsätzlich deutsches Datenschutzrecht, dessen unterschiedliche Standards abhängig von den jeweils betroffenen Daten eingehalten werden müssen.[179] Das deutsche Datenschutzrecht geht grundsätzlich davon aus, dass Daten an genau festgelegten Orten gespeichert werden.[180] Insbesondere dürfen Daten nur in Ausnahmefällen außerhalb Europas übermittelt werden.[181] Genau dies ist jedoch bei weltweit verteilten Serverfarmen mit der Konzeption von Cloud-Computing nicht zu gewährleisten. Gerade in Anbetracht der erheblichen Unterschiede zwischen deutschen und internationalen Datenschutzkonzepten sind Konflikte im Datenschutz unvermeidlich.[182]

Zudem muss die Verarbeitungsanlage, sofern Daten im Anwendungsbereich des BDSG betroffen sind, die weitreichenden organisatorischen und technischen Anforderungen des § 9 BDSG und dessen Anlage entsprechen. So müssen etwa umfassende Zutritts-, Zugangs- und Zugriffskontrollen eingerichtet werden.[183]

Die noch weiter reichende Voraussetzungen des § 11 BDSG (Auftragsdatenverarbeitung) finden Anwendung, wenn die Verarbeitung personenbezogener Daten (Abs. 1) oder auch nur Wartungsarbeiten (Abs. 5) ausgelagert werden. Dies kommt in Betracht, wenn der Cloud-Computing-Anbieter die Daten seiner Kunden an externe Zulieferer auslagert.[184] Sie gelten allerdings auch, wenn Unternehmen ihre Kundendaten in einer

---

[179] Das BDSG richtet sich dabei an die für den Datenumgang verantwortliche, steuernde Stelle. Zur Anwendbarkeit bei grenzüberschreitendem Datenverkehr *Jotzo*, MMR 2009, 232, 233; vgl. BT-Drs. 14/4329, S. 31 f.

[180] Anknüpfungspunkt ist also der körperliche Datenträger, Simitis/*Dammann*, Bundesdatenschutzgesetz, 6. Aufl. 2006, § 3 Rn. 118.

[181] Dies ist möglich, wenn im Drittland ein mit dem hiesigen Datenschutzniveau vergleichbarer Standard herrscht, was z. B. durch EU-Standardvertragsklauseln sichergestellt werden kann, vgl. Gola/Schomerus, BDSG, 9. Aufl. 2007, § 4c Rn. 12; Simitis/*Simitis*, Bundesdatenschutzgesetz, 6. Aufl. 2006, § 4b Rn. 71; *BITKOM*, Cloud Computing - Evolution in der Technik, Revolution im Business, 2009, S. 53.

[182] Vgl. *Spies*, MMR Nr. 5/2009, XI.

[183] Zu den einzelnen Erfordernissen Gola/Schomerus/*Gola*, BDSG, 9. Aufl. 2007, § 9 Rn. 10 ff.

[184] *Karger/Sarre*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 427, 434; *Schulz/Rosenkranz*, ITRB 2009, 232, 234 f.; *Niemann/Paul*, K&R 2009, 444, 449.

Cloud-Computing-Anwendung verwalten, wobei die beauftragenden Unternehmen ggf. eine Erforschungspflicht und die Verpflichtungen aus § 11 Abs. 1 bzw. 2 BDSG trifft, was ebenfalls der Konzeption von Cloud-Computing widerspricht.[185]

Insbesondere Nr. 8 der Anlage zu § 9 BDSG, wonach zu gewährleisten ist, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden,[186] ist bei Cloud-Computing problematisch. Werden Daten auf virtuellen Servern verarbeitet und automatisch zwischen Rechenzentren verteilt, können sich Daten aus unterschiedlichen Quellen in nicht im Einzelnen steuerbarer Weise vermischen. Eine getrennte Verarbeitung kann also nur durch den Einsatz von Verschlüsselungstechnologien gewährleistet werden.[187] Dies ist wohl ausreichend zur Sicherstellung der getrennten Verarbeitbarkeit, was sich aus dem ausdrücklichen Hinweis des Gesetzgebers in Satz 3 der Anlage zu § 9 BDSG bezüglich der Verwendung entsprechender Technologien zur Erfüllung der Erfordernisse der Nummern 2 bis 4 schließen lässt.

Es liegt also an den Betreibern, durch entsprechende Vertragsgestaltung, Betriebsorganisation und Programmierung der Datenverteilung sicherzustellen, dass die strengen Vorgaben des Datenschutzrechts Berücksichtigung finden. Bereits jetzt bieten einige Anbieter an, verarbeitete Daten explizit nur in Europa zu speichern.[188] Auch der Benutzer muss sich des erhöhten Risikos bewusst sein, dass seine Daten gerade bei weltweiten Onlineangeboten unter Umständen nicht den gewohnten datenschutzrechtlichen Schutz genießen.

### *6. Öffentliches Recht*

Nehmen Behörden die Dienste externer Anbieter in Anspruch, handelt es sich wie bei Privaten um eine Auftragsdatenverarbeitung nach § 11 BDSG (bzw. der landesrechtlichen Entsprechung), mit allen damit verbundenen Auswahl- und Überwachungspflichten.[189]

#### *a) Verbot der Mischverwaltung*

Ein Problem könnte sich aus dem Verbot der Mischverwaltung ergeben, welches das BVerfG aus Art. 83 ff. GG herleitet.[190] Demnach sollen die Verwaltung des Bundes und

---

[185] *Karger/Sarre*, in: *Taeger/Wiebe* (Hrsg.), Inside the Cloud, 2009, S. 427.

[186] Vgl. Gola/Schomerus/*Gola*, BDSG, 9. Aufl. 2007, §9 Rn. 29; es bleibt offen, ob eine Trennung virtueller Datenträger den Anforderungen genügen kann.

[187] Vgl. Gola/Schomerus/*Gola*, BDSG, 9. Aufl. 2007, § 9 Rn. 29; *Reppner*, Fakten statt Märchen: Datenschutz in der Cloud, http://www.zdnet.de/it_business_hintergrund_fakten_statt_maerchen_datenschutz_in_der_cloud_story-11000006-41530882-1.htm (Stand: 05.05.2010).

[188] *Schneider*, Handbuch des EDV-Rechts, 4. Aufl. 2009, M Rn. 72.

[189] *Schulz*, MMR 2010, 75, 78.

[190] *BVerfG*, NVwZ 2008, 183, 186; *BVerfG*, NVwZ 1983, 537, 540; *Schulz*, MMR 2010, 75, 76.

die der Länder prinzipiell voneinander getrennt bleiben, wovon auch nicht durch Vereinbarungen oder einfachgesetzliche Vorschriften abgewichen werden kann. Dies bezieht sich allerdings auf Sachentscheidungen bzw. den tatsächlichen Gesetzesvollzug, bei gemeinsamer Nutzung reiner Infrastruktur können Konflikte kaum auftreten. Cloud Computing, sofern es als reine IT-Infrastruktur betrieben wird, ist also nicht vom Verbot der Mischverwaltung erfasst.[191]

*b) Abhängigkeit von privaten Soft-/Hardwareanbietern*

Aus öffentlich-rechtlicher Sicht stellt sich beim Cloud-Computing im verstärkten Maße die Frage, wie weit sich die Verwaltung von privaten Soft- und Hardwareanbietern abhängig machen darf. Wie weit dürfen sensible persönliche Daten auf privaten Servern, oder gar im Ausland gespeichert werden und somit aus dem unmittelbaren Verfügungsbereich der Verwaltung gegeben werden?

Eine Antwort gibt wiederum das Bundesdatenschutzgesetz im zweiten Abschnitt (§§ 12–26 BDSG) bzw. die landesrechtlichen Entsprechungen. Dort werden über die dargestellten Erfordernisse zu technischen Maßnahmen und zur Auftragsdatenverarbeitung hinaus spezielle Vorgaben für die Datenverarbeitung von öffentlichen Stellen vorgesehen, unter anderem Benachrichtigungspflichten und Auskunftsrechte der Betroffenen. Dem steht gegenüber, dass dem Bürger gegenüber der öffentlichen Hand das Instrument der Privatautonomie fehlt, durch das er die Speicherung seiner Daten durch privatrechtliche Unternehmen von vornherein verhindern kann. Abseits der rechtlichen Vorgaben birgt eine Auslagerung auch aus rein tatsächlicher Hinsicht, gerade in Anbetracht des besondere Sicherheitsbedürfnisses und Geheimhaltungsinteresse der Bürgerdaten, gesteigerte Gefahren.

*7. Weitere Aspekte*

Es stellt sich die Frage, ob das Telekommunikationsgesetz (TKG) auch auf Cloud-Computing-Anbieter anzuwenden ist, etwa die Bestimmungen zum Fernmeldegeheimnis (§ 88 TKG) und zum Datenschutz (§§ 91 ff. TKG). Dazu muss der Anbieter Dienstanbieter sein (vgl. §§ 88 Abs. 2 TKG), also geschäftsmäßig Telekommunikationsdienste erbringen (§ 3 Nr. 6a TKG). Dies sind in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen (§ 3 Nr. 24 TKG). Zwar basiert das Konzept Cloud-Computing im Wesentlichen aus der Vernetzung und Datenübertragung zwischen verschiedenen Serversystemen, zur Beurteilung der Eigenschaft als Dienstanbieter im Sinne des TKG ist hier aber lediglich das Außenverhältnis des Anbieters zum Kunden von Bedeutung,[192]

[191] *Schulz*, MMR 2010, 75, 77.
[192] BeckTKG-Komm/*Robert*, 2006, § 3 Rn. 18.

nicht jedoch der Kernbereich des Cloud-Computings hinter den Kulissen, also die Verteilung der Ressourcen und Verarbeitung der Datenströme auf Anbieterseite. Gegenüber dem Endkunden wird gerade keine Telekommunikationsleistung in Form von Signalübertragungen erbracht, sondern lediglich die jeweilige Softwareschnittstelle bereitgestellt.[193] Die Signalübertragung vom Kunden zur Cloud-Computing-Anwendung ist regelmäßig nicht Bestandteil des Leistungsangebots des Cloud-Computing-Anbieters, sondern sind Leistungen der Internet-Service- bzw. Access-Provider. Nur diese sind etwa auch Verpflichtete in Auskunftsverfahren nach § 113 TKG.[194]

### *III. Zusammenfassung*

Die zukünftige Entwicklung lässt sich bereits jetzt abschätzen: Mit steigender Verfügbarkeit dauerhafter Breitbandverbindungen zum globalen Netz, zunehmender Rechenleistung der Server und den wachsenden Mobilitätsansprüchen der Nutzer wird der Trend weiterhin dahin gehen, Betriebssysteme und Software ins Internet auszulagern.[195] Die Anbieter werden – auch im Interesse ihrer Kunden – ein noch genaueres Nutzerprofil erstellen und genau die Dienste anbieten, die der Nutzer benötigt. Dieser wird wiederum auch die persönlichsten Daten auf den Servern der Anbieter hinterlegen und dabei einen erheblichen Vertrauensvorschuss leisten – ist er doch auf die Datensicherheit und Verschlüsselungsmechanismen des jeweiligen Anbieters angewiesen.

Noch ist kein akuter Handlungsbedarf des Gesetzgebers ersichtlich, die aufgeworfenen Probleme erscheinen de lege lata gut lösbar.

---

[193] So auch *Schuster/Reichl*, CR 2010, 38, 43.

[194] BeckTKG-Komm/*Bock*, 2006, § 113 Rn. 2; vgl. *Gercke*/*Brunst*, Praxishandbuch Internetstrafrecht, 2009, Rn. 657.

[195] Etwa Microsoft Azure (hybrides Modell).

# Kapitel 2: Mashups

*P. Thal*

## *I. Begriff und Technologie*

Mashups sind ein ganz klassisches Phänomen des Web 2.0. Im weitesten Sinne versteht man darunter die Verbindung und Vermischung bereits bestehender Webinhalte zu einer neuen, innovativen Webanwendung. So ist es z.B. möglich, GoogleMaps mit eigenen oder fremden Contents zu kombinieren, um einen neuen Webinhalt zu schaffen. Denkbar wäre dies in der Form, dass man mithilfe von GoogleMaps und einer Kriminalstatistik einen Dienst anbietet, der auf einer Karte anzeigt, in welcher Gegend einer Stadt besonders viele Verbrechen begangen werden.[196] Dieses Prinzip lässt sich beliebig vervielfachen, indem man die „Verbrechen" mit „Singles in deiner Umgebung" oder „Freie Parkplätze in deiner Umgebung" austauscht.[197] Auf diese Art und Weise wird es viel einfacher, neue kreative Dienste zu schaffen, zumal nur relativ simple Programmierstrukturen für eine solche Kombination erforderlich sind. Ursprünglich stammt der Begriff aus dem Bereich der Musik und beschreibt dort das Vermischen von bekannten Musikstücken zu einem neuen sog. „Remix" oder „Sampling".[198] Für das Web 2.0 erlangt der Begriff vor allem deswegen Bedeutung, weil die veränderte Rollenverteilung beim Erstellen von Webinhalten zu einer eben solchen Vermischung geführt hat: Nicht mehr nur die großen Online-Dienste, sondern auch die einzelnen User stellen verschiedene Contents ins Internet und sind dabei häufig auf vorprogrammierte Schnittstellen der jeweiligen Anbieter angewiesen.

Diese Schnittstellen, sog. APIs[199], sind der Dreh- und Angelpunkt der Mashup-Technologie. Ebenso wie auch ein Betriebssystem für verschiedene Anwendungen (Zugang zum Dateisystem, Zugang zum Netzwerk, Zugriff auf Programme) verschiedene Programmierschnittstellen vorsieht, so besteht auch das Internet aus einzelnen Berührungspunkten, mittels derer eine Kommunikation zwischen verschiedenen Prozessen oder Komponenten stattfinden kann. Anbieter wie Yahoo, Ebay, Amazon oder Google können nun einzelne ihrer Schnittstellen dergestalt programmieren und freigeben, dass Dritte darauf zugreifen und sie verwenden können. Die Erstellung des Mashups selbst richtet sich i.d.R. nach den Vorgaben des jeweiligen Anbieters der API, der für die Verbindung seiner Schnittstelle mit einem anderen Content entweder eine grafische Benut-

[196] Siehe „Chicago Crime Map", http://www.chicagocrime.org (01.05.2010).
[197] Diese Geschäftsmodelle wurden schon von den Firmen *frozenbear* und *parkingcarma* verwendet.
[198] *Holz*, HMD Praxis der Wirtschaftsinformatik 2007, S. 70.
[199] Application programming interfaces.

zerfläche bereit stellt oder aber die Verwendung bestimmter Netzwerkprotokolle voraussetzt. Oftmals ergeben sich die erforderlichen technischen Bedingungen auch aus der Eigenart des geplanten Mashups (z.B. Videomashups)[200].

### *II. Arten von Mashups*

Differenzieren kann man die verschiedenen Arten von Mashups anhand ihrer Zielrichtung bzw. –gruppe. So dienen Verbrauchermashups vorwiegend dazu, bestimmten Konsumentengruppen Informationen über Produkte oder Dienstleistungen zukommen zu lassen oder ihnen die Möglichkeit zu geben, sich selbst Mashups von beliebten Websites zu erstellen.[201] Video-Mashups verbinden Audio- oder Videodateien miteinander und formen so ein neues künstlerisches Werk. Datenmashups sind hingegen bloße Verbindungen von zwei oder mehreren unabhängigen Datensätzen, die im neuen „Mashupgewand" einem anderen als dem ursprünglichen Zweck zugeführt werden. Dies ist z.B. bei den oben beschriebenen GoogleMaps-Mashups der Fall, die insoweit bloße Darstellungen sind.[202] Unternehmerische Mashups zielen ebenso auf die Darstellung von Informationen aus verschiedenen Quellen ab, ermöglichen gleichzeitig aber auch die Zusammenarbeit und Weiterentwicklung von den daran beteiligten Unternehmen mithilfe komplexerer Software, wobei hier anders als bei den Verbrauchermashups Datensicherheit und –zuverlässigkeit, Performance und Skalierbarkeit eine große Rolle spielen.[203]

### *III. Rechtliche Bewertung*

Die rechtlichen Problemfelder von Mashups sind ebenso vielfältig wie die Mashup-Kultur selbst: Herausforderungen stellen insoweit sowohl das Vertrags- und Urheberrecht, als auch das Marken- und Patentrecht dar. Gleiches gilt – wenn das Mashup entsprechend ausgestaltet wird – auch für das Strafrecht. Der klassische Fall eines reinen Datenmashups erfasst insoweit die meisten rechtlichen Probleme, sodass anhand dieses Regelfalls die rechtliche Beurteilung stattfinden soll.

---

[200] Siehe hierzu unten: Kapitel I – II.

[201] Sog. consumer mashups; Beispiele hierfür sind (bzw. waren) der Intel Mash Maker, Google Mash Editor und Yahoo Pipes, wobei diese auch von Firmen unter Zuhilfenahme eines Mashup-Servers als enterprise mashups verwendet werden können; siehe zu einem weiteren Verständnis von consumer mashups: http://searchcrm.techtarget.com/feature/Consumer-and-enterprise-mashups (01.05.2010).

[202] Sog. data mashups; weitere Beispiele finden sich unter www.housingmaps.com, www.flashearth.com und www.wayfaring.com und www.musicportl.com.

[203] Sog. enterprise mashups; siehe hierzu: http://wiki.computerwoche.de/doku.php/web_2.0/enterprise-mashups; z.B. Convertigo Mashup und Kapow Mashup.

### *1. Strafrechtliche Dimensionen*

Verbindet ein privater User bereits bestehende Daten aus dem Web zu einem neuen Werk[204], ist erst einmal noch nichts Kriminelles geschehen. Kommt aber zu diesem neutralen Verhalten eine „böse Gesinnung" hinzu, die sich auch objektiv im Werk manifestiert, kann die Handlung strafrechtlich relevant werden. Denkbar wäre das z.B. dann, wenn ein User das Kartenmaterial von Google-Maps verwendet, um darauf kompromittierende oder ehrverletzende Äußerungen über seine Nachbarn, die Restaurants in der Umgebung oder andere ihm bekannte Personen oder Institutionen zu tätigen.

Solche „Bewertungsplattformen" finden sich im Web in den unterschiedlichsten Ausgestaltungen. Während manche Plattformen relativ seriös über ein Thema oder eine Personengruppe berichten und Bewertungen diesbezüglich ermöglichen (spickmich.de, meinprof.de) [205], gleichen manch andere Plattformen eher einer modernen Hexenjagd[206]. Dies ist z.B. der Fall beim amerikanischen Portal rottenneighbor.com, welches mittlerweile für deutsche Internetuser nicht mehr erreichbar ist.[207] Hier wurde bis zur Auflösung der Seite im Juni 2009 das Kartenmaterial von GoogleMaps dafür verwendet, lästige Nachbarn öffentlich zu denunzieren. Zwar bestand auch die Möglichkeit, die Karte mit „grünen", d.h. „positiven", Markern zu versehen, was allerdings weitaus weniger genutzt wurde. In der Folge waren dann Bewertungen wie „N verkauft heimlich Drogen an Jugendliche" und „B ist ein glatzköpfiger Alkoholsüchtiger, der morgens schon säuft" auf der Seite zu lesen.[208]

Wird ein Mashup auf diese Weise genutzt, kommen gleich mehrere Straftatbestände in Betracht. Sowohl der klassische § 185 StGB als auch die §§ 186, 187 StGB können erfüllt sein. Im ersten Fall ist erforderlich, dass der Täter gegenüber dem Betroffenen ehrenrührende Tatsachen oder gegenüber einem Dritten oder dem Betroffenen ehrenrührende Werturteile geäußert hat. Eine solche Kundgabe von Missachtung ist aber i.d.R. nicht gegeben, wenn eine Tatsache erweislich wahr ist. Als ungeschriebenes Tatbestandsmerkmal ergänzt daher die „Unwahrheit der Tatsachenbehauptung" den objektiven Tatbestand. In den Fällen der §§ 186, 187 StGB muss der Täter auch eine unzutreffende Tatsache geäußert haben, wobei hier aber nur die Kundgabe gegenüber Dritten erfasst ist. Im Falle des § 187 StGB kommt hinzu, dass sich der Täter dieser Unwahrheit bewusst gewesen sein muss. Nach h.M. ist die Unwahrheit der Äußerung bei

---

[204] Siehe hierzu unten: 2. c) aa).

[205] Die Bewertungsplattform spickmich.de wurde schon vielerorts kontrovers diskutiert. Zugleich befassten sich auch die Gerichte mit der Plattform und deren Zulässigkeit: BGH NJW 2009, 2888 ff.

[206] *Graef*, ZUM 2009, 759.

[207] Zwischenzeitlich war das Portal nur für deutsche User gesperrt, nachdem immer mehr Stimmen aufkamen, die die Zulässigkeit von rottenneighbor.com anzweifelten.

[208] http://www.focus.de/digital/internet/rotten-neighbor-internetpranger-teilweise-offline_aid_329975.html.

§ 186 StGB nur objektive Bedingung der Strafbarkeit, sodass sich der Vorsatz des Täters nicht darauf beziehen muss.[209]

Solange es sich nur um Meinungsäußerungen handelt, die in Datenmashups preisgegeben werden, kommt nur § 185 StGB in Betracht. Die Grenze zwischen bloßer Kritik und ehrverletzender Kundgabe von Missachtung ist dabei nicht leicht zu ziehen. Allein der Umstand, dass die im Internet getroffene Aussage einer breiten Öffentlichkeit zugänglich ist, rechtfertigt indes noch nicht die Annahme des § 185 StGB.[210] Gleiches gilt auch für den freilich problematischen Regelfall, dass Gegenmaßnahmen des Opfers mangels Kenntnis oftmals nicht ergriffen werden können.[211] Anders als eine Bewertung von Lehrern im Internet betreffen die Aussagen im rottenneighbor.com-Portal aber nicht lediglich die Sozialsphäre der Opfer, sondern deren Intim- und Privatsphäre, indem sie deren Lebensweisen und Wohnverhältnisse offenlegen und kritisieren. Durch diese Äußerungen entsteht eine soziale Ausgrenzung in der Form, dass andere Nachbarn über die vermeintlich wahren Umstände aufgeklärt werden und ihre eigenen – leicht vorherzusehenden – Schlüsse daraus ziehen. Auch eine Art Prangerwirkung lässt sich nicht ausschließen, zumal ein schutzwürdiges Informationsinteresse der Allgemeinheit über die privaten Lebensumstände nicht ersichtlich ist, sodass die Zurschaustellung des Opfers in den Mittelpunkt rückt. Ähnlich sah es auch der BGH in einer zivilrechtlichen Entscheidung[212] zur Bewertungsplattform „spickmich.de“, wonach Äußerungen im Rahmen der Sozialsphäre des Betroffenen nur im Falle schwerwiegender Auswirkungen auf das Persönlichkeitsrecht mit negativen Sanktionen verknüpft werden dürfen, so etwa dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu erwarten ist. Diese Wertungen des Zivilurteils überzeugen vor dem Hintergrund des „in dubio pro reo“-Grundsatzes und der gebotenen engen Auslegung des § 185 StGB auch aus strafrechtlicher Sicht: Zum einen korreliert der Ehrbegriff ohnehin mit dem Begriff des allgemeinen Persönlichkeitsrechts.[213] Bei dem § 185 StGB findet zwar keine klassische Interessenabwägung in der oben genannten Form statt. Dennoch sind alle Begleitumstände mit einzubeziehen, die die Äußerung zur Missachtung des ethisch-moralischen Werts des Betroffenen machen. Insoweit ist der § 185 StGB auch nicht auf Fälle beschränkt, in denen nur privateste Umstände des Betroffenen Gegenstand der Äußerung sind.[214]

---

[209] *Fischer*, StGB, § 186 Rn. 13.

[210] *Beck,* MMR 2009, 736 (737).

[211] Vgl. „Kampf gegen das Online-Mobbing“: http://www.focus.de/digital/internet/internet_aid_237343.html (Januar 2010); *Beck*, MMR 2009, 736 (737).

[212] BGH NJW 2009, 2888, 288.

[213] Siehe hierzu: *Beck,* MMR 2009, 736, 737.

[214] Im Übrigen gilt es auch das Urheberstrafrecht zu beachten, vgl. §§ 106 ff. UrhG.

### *2. Zivilrechtliche Dimensionen*

#### *a) Vertragsrecht*

Im zivilrechtlichen Bereich sind die relevanten Problemfelder noch facettenreicher. Zum einen bildet das Vertragsrecht eine erste rechtliche Hürde. Die Nutzung der APIs wird regelmäßig durch einen Lizenzierungsvertrag geregelt, unabhängig davon, ob die Zurverfügungstellung gegen Entgelt oder gratis erfolgt.[215] Diese Verträge enthalten regelmäßig Einzelheiten über die Zurverfügungstellung der APIs, wie z.B. Platzierung von Werbebannern, Umfang von Aufklärungspflichten oder Haftungsfragen.[216] Interessant sind aber vor allem die Klauseln, die nur eine „nicht wirtschaftliche Nutzung" des API-Dienstes vorschreiben.[217] Je nach Ausgestaltung der Klausel kann es dann einer Partei (API-Inhaber und API-Betreiber) untersagt sein, Werbung zur Finanzierung des Webdienstes einzusetzen oder das API auf einer bereits bestehenden Website mit geschäftlichen Angeboten zu verwenden.[218]

#### *b) Markenrecht*

Aus markenrechtlicher Sicht sind Mashups insoweit interessant, als dass sie regelmäßig auf zumindest einen fremden Inhalt zurückgreifen und verweisen müssen, der u.U. markenrechtlich geschützte Elemente enthalten kann.[219] Werden nach Entstehung des Markenschutzes (§ 4 MarkenG) die Kennzeichnungsrechte verletzt, kann dieser gegen den Mashup-Betreiber entweder Unterlassungsansprüche (§§ 14 Abs. 5; 15 Abs. 4 MarkenG) oder Schadenersatzansprüche (§§ 14 Abs. 6; 15 Abs. 5 u. Abs. 6 i.V.m. § 14 Abs. 7 MarkenG) geltend machen. Wann eine solche Verletzung von Markenrechten gegeben ist, wird durch § 14 Abs. 2 MarkenG geregelt. Danach ist es Dritten untersagt, prioritätsjüngere identische (Nr. 1) oder ähnliche (Nr. 2,3) Marken zu benutzen. Zum Teil sind noch weitere Voraussetzungen wie die „Verwechslungsgefahr" nach Nr. 2 oder die „Ausnutzung der Wertschätzung der bekannten Marke in unlauterer Weise" nach Nr. 3 zu prüfen. Gemeinsam ist den Tatbeständen aber, dass die Benutzung der Marke „im geschäftlichen Verkehr" erfolgen muss. Es stellt sich insoweit ein ähnliches Problem wie schon im Vertragsrecht: Bei Mashups ist eine „wirtschaftliche Nutzung" oder ein „Handeln im geschäftlichen Verkehr" keineswegs von vorherein zu bejahen. Allein der Umstand, dass die erstellten Mashup-Dienste im Internet für eine breite Öffentlichkeit frei zugänglich sind, rechtfertigt eine irgendwie geartete „wirtschaftliche Nutzung" freilich noch nicht. Erforderlich ist vielmehr, dass eine

---

[215] *Ott,* K & R 2007, 623 (624).

[216] Siehe hierzu das Google Maps API premier purchase agreement: http://support.google.com/enterprise/doc/gme/terms/maps_purchase_agreement.html.

[217] Siehe hierzu schon: *Ott*, K & R 2007, 623 (624).

[218] Siehe hierzu unten näher: 2. b) und c).

[219] *Ott*, K & R 2007, 623 (626).

wirtschaftliche Tätigkeit auf dem Markt erfolgt, die der Förderung eines eigenen oder fremden Geschäftszwecks zu dienen bestimmt ist.[220] Wenn die Enduser-Nutzung des Mashups kostenpflichtig ausgestaltet wird, kann diese Voraussetzung unproblematisch angenommen werden.

In der Regel ist dies aber gerade nicht der Fall, weil schon die jeweiligen Nutzungsbedingungen bzw. Lizenzierungsverträge für die API-Nutzung vorsehen, dass der daraus erstellte Mashup-Dienst Dritten kostenlos zur Verfügung gestellt werden muss. Unter Punkt 10.3 der Nutzungsbedingungen für die GoogleMaps-API etwa findet man die Bestimmung: „[…] you must not (nor may you permit anyone else to) […] charge users or any other third party any fee for the use of the Maps API implementation [….]".[221] Bei Flickr.com wird schon auf der Eingangsseite zur API-Nutzung darauf hingewiesen, dass die Flickr-API von anderen Entwicklern nicht zu „kommerziellen Zwecken" verwendet werden darf.[222] Ebay schreibt in seinem Lizenzierungsvertrag dem Mashup-Betreiber vor: „All fees due (if any) for all API calls initiated by Your Users will be paid by you".[223] All dies legt den Schluss nahe, dass eine "Nutzung im geschäftlichen Verkehr" i.S.d. § 14 Abs. 2 MarkenG regelmäßig nicht vorliegen wird, solange sich die Mashup-Betreiber vertragsgemäß (im Bezug auf den API-Anbieter) verhalten.

Andererseits machen auch die oben genannten Lizenzierungsverträge eine Ausnahme, wenn sie „anderweitige Vereinbarungen zur kommerziellen Nutzung" ermöglichen.[224] Zu beachten gilt es ferner, dass viele Mashup-Betreiber ihre laufenden Kosten mit Werbeeinnahmen finanzieren, die sie durch entsprechende Ausgestaltung der Werbebanner ihrer Website erzielen. Im Übrigen ist der Begriff des „Handels im geschäftlichen Verkehr" nach h.M. weit auszulegen und liegt mithin schon dann vor, wenn die Benutzung des Kennzeichens im Zusammenhang mit einer auf einen wirtschaftlichen Vorteil gerichteten, kommerziellen Tätigkeit und *nicht im privaten Bereich* erfolgt.[225] Diese Grundsätze gelten nach der Rechtsprechung des BGH auch im Bereich des Internets, sodass auch im Rahmen von Mashups keine hohen Anforderungen an den Begriff des „geschäftlichen Verkehrs" zu stellen sind. Aufgrund der Vielfältigkeit der Mashup-Kultur sind zwar durchaus auch Konstellationen denkbar, in denen keine kommerzielle Nutzung im Sinne des § 14 Abs. 2 MarkenG vorliegt. Angesichts der Tatsache, dass die wenigsten Mashups nur im privaten Bereich erfolgen, wird man in den meisten Fällen

---

[220] BGH GRUR 2004, 241 (242); OLG Köln NJWE-WettbR 2000, 242 (242); *Ingerl/Rohnke*, § 14 Rn. 35 ff.; *Nordemann*, Wettbewerbsrecht-Markenrecht, Rn. 2281 f.

[221] http://code.google.com/intl/de-DE/apis/maps/terms.html (Januar 2010).

[222] http://www.flickr.com/services/api/ (Januar 2010).

[223] http://developer.ebay.com/join/licenses/individual/ Punkt 9.2.4 (Januar 2010).

[224] http://www.flickr.com/services/api/ (Januar 2010); http://code.google.com/intl/de-DE/apis/maps/terms.html unter Punkt 9.2.4.(Januar 2010).

[225] BGH GRUR 2008, 702 (705); *Fezer*, § 14 Rn. 25; Ströbele/Hacker/*Hacker*, § 14 Rn. 27.

ein Handeln im geschäftlichen Verkehr bejahen können. Dementsprechend kann es dazu kommen, dass – sofern die Lizenzierungsverträge von einem engeren Verständnis der kommerziellen Nutzung ausgehen – der Mashup-Betreiber nach dem MarkenG im „geschäftlichen Verkehr handelt", ohne gleichzeitig auch gegen seinen Lizenzierungsvertrag zu verstoßen.

### *c) Urheberrecht*

Im Urheberrecht können vor allem die §§ 97 Abs. 1, 19a, 23 UrhG relevant werden. Demnach hat der Rechtsinhaber Ansprüche auf Unterlassung und Schadensersatz, wenn *das geschützte Werk öffentlich zugänglich gemacht (§ 19a UrhG) oder bearbeitet* (§ 23 UrhG) wird. Damit ist der klassische Fall von Mashups beschrieben, bei denen bestehende Webinhalte mit anderen Contents verbunden und dann im Internet öffentlich zugänglich gemacht werden.

#### *aa) Werkqualität*

Fraglich ist aber, ob die API als bloße Programmierschnittstelle als „Werk" im Sinne der §§ 1, 2 UrhG angesehen werden können. Im UrhG finden sich einige Anhaltspunkte, die dafür sprechen, dass die API urheberrechtlich geschützt ist:

Unproblematisch sind zunächst die Fälle, in denen der API Kartenmaterial, Pläne oder Skizzen zu Grunde liegen oder ihr sonst angehören. Solche Teile der API bilden selbst eine eigene Werkgattung und können daher eindeutig dem § 2 UrhG zugeordnet werden. Ferner wird innerhalb der §§ 1, 2 UrhG vertreten, dass auch die Website als Zusammensetzung von Leistungen aus bekannten Werkgattungen als Werk anzusehen ist, obgleich es sich um keine neue Werkgattung handelt.[226] Die einzelnen Bestandteile einer Website können regelmäßig einzelnen Werkgattungen zugeordnet werden und hierüber den Schutz des UrhG erfahren. So kann etwa bei Vorliegen einer entsprechenden Schöpfungshöhe die graphische Gestaltung der Website als Werk der angewandten Kunst verstanden werden. Auch die Struktur der Benutzeroberfläche kann nach § 2 Abs. 1 Nr. 7 UrhG Werkqualität aufweisen.[227] Bei APIs gilt es allerdings zu beachten, dass sie in der Regel nicht nur als Darstellungen (wie Websiteelemente) auf der Mashup-Website vertreten sind, sondern in der Regel auch gewisse Datenverarbeitungsprozesse durchführen. Eine solche Befehls- und Steuerungsfunktion ist kennzeichnend für den Begriff der Computerprogramme, wie er in § 2 Abs. 1 Nr. 1 i.V.m. § 69a UrhG Niederschlag gefunden hat.[228] Aufgrund der Vielzahl der Ausgestaltungsmöglich-

---

[226] Dreyer/Kotthoff/Meckel/*Dreyer,* § 2 Rn. 275.

[227] Dreyer/Kotthoff/Meckel/*Dreyer,* § 2 Rn. 275; Plaß, WRP 2000, 599 (600 f.).

[228] Vgl. zur Definition vom BGH: „… eine Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind, zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder

keiten von APIs und den ihr zu Grunde liegenden Daten, sind sie entweder alleine nach § 2 UrhG oder i.V.m. mit § 69a UrhG als urheberrechtlich geschütztes Werk zu qualifizieren.

*bb) Kein Nutzungsrecht durch Einwilligung*

Zu einer tatsächlichen Verletzung von urheberrechtlich geschützten Werken kann es aber erst dann kommen, wenn eine Einwilligung des Rechtsinhabers nicht vorliegt. So fordert etwa § 23 UrhG, dass Bearbeitungen oder andere Umgestaltungen des Werkes „nur mit Einwilligung" des Urhebers erfolgen dürfen. Ähnlich liegt dies auch bei § 97 UrhG, der für das Vorliegen eines Unterlassungs- oder Schadensersatzanspruchs die „Widerrechtlichkeit" der Urheberrechtsverletzung fordert. Diese ist regelmäßig dann zu bejahen, wenn der Verletzer gerechtfertigt ist, namentlich dann, wenn der Rechtsinhaber in die Benutzungshandlung eingewilligt oder sie genehmigt hat.[229]

Bei § 23 UrhG kann die Einwilligung auch in der Vergabe der Lizenz am Originalwerk gesehen werden. Hat der Urheber mit einem Dritten einen Lizenzierungsvertrag geschlossen, ist durch Auslegung zu ermitteln, ob er auch die Einwilligungsrechte nach § 23 UrhG enthalten soll.[230] Damit ist aber der Fall beschrieben, in dem der Dritte nicht nur die Lizenz, sondern auch selbst das Recht zur Erteilung der Einwilligung gegenüber anderen erhalten soll. Der Dritte (bzw. der spätere Verletzer) selbst aber erhält eine Einwilligung regelmäßig dadurch, dass er mit dem Urheber einen bloßen Nutzungsvertrag abgeschlossen hat.[231] Diese Einräumung gegenständlicher Nutzungsrechte an dem am Originalwerk bestehenden Urheberrecht ist aber nach Inhalt und Umfang nicht ohne weiteres aus dem Vertrag ersichtlich. Als Auslegungshilfe bestimmt die sog. Zweckübertragungslehre die Situationsbezogenheit der Einwilligung, d.h. ihre Geltung besteht nur in den Grenzen des Kontextes, in dem sie erteilt wurde. [232] Ihre konkrete Reichweite ist somit durch Interessenabwägung zu ermitteln, wobei die urheberpersönlichkeitsrechtlichen Interessen des Urhebers, wie sie in § 14 UrhG Ausdruck gefunden haben, zu berücksichtigen sind.[233]

Für den Mashup-Bereich lässt sich damit zusammenfassen: Der API-Inhaber und der Mashup-Betreiber schließen regelmäßig Lizenzierungsverträge, in denen auch die Nutzung der Schnittstelle geregelt ist. Schon allein dadurch erhält der Mashup-Betreiber die Befugnis zur Nutzung und Bearbeitung der API. Schließlich ist für ein Mashup schon

---

erzielt." BGH GRUR 1985, 1041, 1047; Dreyer/Kotthoff/Meckel/*Kotthoff,* § 69a Rn. 4.

[229] BGH GRUR 1959, 147 (149); Dreyer/Kotthoff/Meckel/*Meckel*, § 97 Rn. 34.

[230] Dreyer/Kotthoff/Meckel/*Dreyer,* § 23 Rn. 23.

[231] Dreyer/Kotthoff/Meckel/*Dreyer,* § 23 Rn. 24.

[232] BGH NJW 1987, 1404; Dreyer/Kotthoff/Meckel/*Dreyer,* §23 Rn. 26; *Fromm/Nordemann,* § 23 Rn. 3; *Schricker/Loewenheim*, § 23 Rn. 20.

[233] Dreyer/Kotthoff/Meckel/*Dreyer*, § 23 Rn. 26.

begrifflich vorauszusetzen, dass zwei Webinhalte miteinander verbunden und insoweit auch „umgestaltet“ bzw. „bearbeitet“ werden (vgl. § 23 UrhG). Allerdings gilt diese Nutzung der APIs – wie bereits oben gesehen – nicht uneingeschränkt. Oftmals werden bestimmte Nutzungsarten ganz konkret untersagt oder aber abstrakt für unzulässig erklärt, wie etwa die „kommerzielle Nutzung“ der API. Für den Fall, dass der Mashup-Betreiber diese vertragliche Regelung verletzt und für die Nutzung seines Dienstes von Dritten Entgelt verlangt, ist die Wirksamkeit dieser einmal erteilten Einwilligung erneut zu prüfen: Die Einwilligung ist zunächst nicht schon deshalb unwirksam, weil der Nutzungs- und Lizenzierungsvertrag durch das vertragswidrige Verhalten „unwirksam“ geworden ist. Zwar mag der API-Inhaber von dem Vertrag zurücktreten oder ihn u.U. sogar anfechten können; allerdings bedarf es dann einer entsprechenden Gestaltungserklärung. Letztlich kommt es aber darauf gar nicht mehr an, wenn die Einwilligung schon aus anderen Gründen unwirksam ist. Betrachtet man den Lizenzierungs- und Nutzungsvertrag als Gesamtgebilde und unterstellt, dass der API-Inhaber die Nutzung und damit die Einwilligung (aus urheberrechtlicher Sicht) von vornherein an die für ihn besonders wichtige „Bedingung“ knüpfen will, dass die Enduser-Nutzung des Mashups kostenlos erfolgen soll, könnte man schon den *Umfang der Einwilligung* dahingehend einschränken, dass sie nur so weit reichen soll, wie eine nicht-kommerzielle Nutzung des Mashups erfolgt. Fraglich ist aber, ob gerade die Wertungen des Urheberrechts für dieses Ergebnis sprechen, sodass auch die Rechtsfolgen des UrhG Wirkung entfalten. Schließlich bietet ja auch die Vertragsverletzung an sich eine ausreichende Anspruchsgrundlage für den API-Inhaber, der dann gem. §§ 280 ff. BGB und §§ 323 ff. BGB vorgehen kann. Anders formuliert: Soll der Mashup-Betreiber dann überhaupt oder auch wegen einer Urheberrechtsverletzung auf Unterlassung und Schadensersatz verklagt werden können? Hierauf wird man erwidern können, dass es sich bei dem Fehlverhalten des Mashup-Betreibers, der entgegen dem Nutzungsvertrag einen kostenpflichtigen Dienst anbietet, nicht um eine spezifisch urheberrechtliche „Angriffsmaßnahme“ handelt. Vielmehr führt eine typisch vertragsrechtliche Pflichtverletzung dazu, dass durch entsprechende Auslegung der Einwilligung urheberrechtliche Unterlassungs- und Schadensersatzansprüche entstehen können.

#### *cc) Zwischenergebnis*

Zusammenfassend lässt sich festhalten, dass der Mashup-Betreiber regelmäßig Werke im Sinne des UrhG miteinander verbindet und insoweit auch entsprechend §§ 23, 19a UrhG handelt. Allerdings ist im Lizenzierungsvertrag zwischen API-Inhaber und Mashup-Betreiber regelmäßig eine Einwilligung zu eben diesem Verhalten enthalten. Je nach Ausgestaltung des Vertrages kann aber der Umfang der Einwilligung derart

beschränkt sein, dass ein vertragswidriges Verhalten des Mashup-Betreibers zu einer urheberrechtlichen Verletzungshandlung führen kann.[234]

### *IV. Schlussbetrachtungen*

Die ausgewählten Problemfelder haben gezeigt, dass eine einheitliche rechtliche Beurteilung von Mashups nur schwer stattfinden kann. Die vielfältigen Ausgestaltungsmöglichkeiten und Erscheinungsformen der vermischten Webinhalte zwingen vielmehr zu einer Einzelfallbetrachtung, wobei auch abstrakte Leitlinien erkennbar werden: Im Strafrecht bilden Mashups ein neues Format um klassische Straftatbestände zu begehen, wobei die Besonderheiten des Internets auch hier Berücksichtigung finden.[235] Die Bestimmungen in den Lizenzierungs- und Benutzungsverträgen von APIs beeinflussen weitaus mehr als das bloße vertragliche Verhältnis zwischen API-Inhaber und Mashup-Betreiber. Sowohl im Marken- als auch im Urheberrecht treffen Mashups auf das Spannungsverhältnis zwischen privater und kommerzieller Nutzung in seiner jeweiligen, rechtsspezifischen Ausprägung. Wie schon vielerorts erwähnt[236], hinkt das Internetrecht der rasanten technischen Entwicklung tatsächlich hinterher. Unklarheiten entstehen vor allem dort, wo lückenhafte vertragliche Regelungen auf modernste technische Sachverhalte treffen, die in ihrer konkreten Form noch nicht diskutiert wurden. Eine ausführliche und detaillierte Ausarbeitung von Lizenzierungs- und Benutzungsverträgen gewinnt damit einmal mehr an Bedeutung.

[234] Siehe zum Haftungsrecht (insbesondere der Metasuchmaschinen) *Ott*, K & R 2007, 623 (626).
[235] Siehe hierzu eingehend: *Beck,* MMR 2009, 736 ff.
[236] Z.B. *Ott,* K & R 2007, 623 (628).

# Kapitel 3: Identitätsdiebstahl im Web 2.0 am Beispiel der sozialen Netzwerke

*R. Nobis*

## *I. Einführung*

Das Web 2.0 ist gekennzeichnet durch eine veränderte Wahrnehmung und Nutzung des Internets seitens der Benutzer. Der Internetnutzer ist nicht länger nur mehr Konsument, sondern er generiert und bearbeitet Inhalte selbst und stellt diese über das Internet zur Verfügung. Der Hintergrund für diese Bewegung zeigt sich in dem gesteigerten Kommunikations- und Partizipationswillen der User. Internetnutzer wollen eigene Inhalte erstellen und mit anderen Personen in Kontakt treten.

Gesellschaftliche Bedeutung erlangt dieses Phänomen insbesondere durch die sozialen Netzwerke. Mittlerweile gehören sie zu den meistgenutzten Kommunikationsmitteln im Internet. Soziale Netzwerke sind eine Anwendung des Web 2.0 und legen den Grundstein für eine Vernetzung und Kommunikation der Menschen in der digitalen Welt. Ihre Nutzung dient der Kommunikation, der Kontaktpflege und dem Informationsaustausch mit anderen Usern.[237] Eine Vernetzung erfolgt in der Weise, dass Mitglieder nach einer Registrierung ein Profil mit allgemeinen und personenbezogenen Daten erstellen, Kontaktlisten anlegen und durch Nachrichten, durch sog. „Pinnwand Einträge“ oder durch Status-Meldungen den Kontakt zu anderen Personen aufbauen und unterhalten. Die sozialen Netzwerke stoßen seitens der Internetnutzer allgemein auf großes Interesse. Viele Millionen Menschen haben sich bereits in ihnen zusammengefunden. Zu den größten Netzwerken zählen inzwischen Facebook mit weltweit über 400 Millionen Mitgliedern[238] und die VZnet Netzwerke (u.a. StudiVZ) mit europaweit 16 Millionen registrierten Nutzern.[239] Hieraus lässt sich ableiten, dass die sozialen Netzwerke eines der wichtigsten und weitreichendsten Phänomene des Web 2.0 darstellen. Dennoch beinhaltet dieser Bereich des Internets zugleich auch Gefahren.

Noch nie zuvor wurden so detailliert und kategorisiert private personenbezogene Informationen von Nutzern zusammengetragen und veröffentlicht. Zwar sind diese Daten im World Wide Web nicht frei verfügbar. Dennoch genügt in allen großen Netzwerken eine einfache Registrierung, um Eingang in die Welt der digitalen Gemeinschaften zu finden. Die innerhalb des Netzwerkes frei verfügbaren Daten sind sodann einsehbar. Die Betreiber der Portale haben von Beginn an datenschutzrechtliche Maßnahmen er-

[237] Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, Privatsphäre in sozialen Netzwerken schützen – Anbieter in die Pflicht nehmen, Deutscher Bundestag, Drucksache 16/11920.

[238] http://www.facebook.com/press/info.php?statistics.

[239] http://static.pe.studivz.net/media/de/pm/100122_2.pdf.

griffen und bieten den Nutzern verschiedene Möglichkeiten, den Zugriff auf ihre Profilseiten einzuschränken. Dies reicht sogar soweit, dass der Nutzer seine Profilseite völlig sperren kann. In einer Welt der digitalen Kontakte, in der zugleich eine erhöhte Kommunikationsoffenheit zu beobachten ist, ist die Hemmschwelle jedoch ziemlich niedrig. Der Erfolg der sozialen Netzwerke und die Möglichkeiten, die sie den Mitgliedern zur Entfaltung ihrer Persönlichkeit im Netz bieten, führen zu einem veränderten Bewusstsein in Bezug auf den Umgang mit personenbezogenen Daten im Internet. Es ist überraschend, wie leichtfertig und naiv viele Mitglieder mit ihren privaten Daten umgehen. Vor allem viele junge Menschen schränken die Einsicht auf ihre Profilseiten kaum bis gar nicht ein. Denn die Interaktion zwischen Menschen erzeugt das Bedürfnis, einander identifizierbar und bezeichenbar zu machen.[240] Begünstigt wird diese Situation auch durch das immer noch zu leichtfertige Umgehen der Portalbetreiber mit den datenschutzrechtlichen Bestimmungen. So sind teilweise die Nutzungsfunktionen so voreingestellt, dass das Profil des Einzelnen für jeden registrierten Nutzer uneingeschränkt einsehbar ist.

Dies zeigt, warum inzwischen mehr personenbezogene Daten im Internet auffindbar sind, als jemals zuvor. Diese Offenheit bezüglich des Umgangs mit sensiblen Informationen im Internet bietet viele Möglichkeiten für einen Missbrauch personenbezogener Daten von Mitgliedern in sozialen Netzwerken. An vorderster Front steht hier der Identitätsdiebstahl.

## *II. Begriff*

Als Identitätsdiebstahl wird im Allgemeinen die missbräuchliche Nutzung personenbezogener Daten einer Person durch Dritte bezeichnet.[241] Die Intention hinter der missbräuchlichen Nutzung liegt in vielen Fällen in der Erlangung eines Vermögensvorteils durch Betrug oder Weiterveräußerung der erlangten Daten an Dritte oder aber darin, die betroffene Person durch bestimmte Verwendung der Informationen in Misskredit zu bringen.[242] Ein Identitätsdiebstahl kann in verschiedenen Ausformungen auftreten. So zeigen sich die häufigsten Formen im Kreditkarten- und Bankbetrug.[243] Insbesondere im elektronischen Geschäftsverkehr – z.B. bei der Durchführung von Transaktionen – kann

[240] Vgl. in diesem Zusammenhang *Rost/Meints*, Authentisierung in Sozialsystemen – Identitytheft strukturell betrachtet, DuD 2005, S. 216.

[241] Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 22. Tätigkeitsbericht, Deutscher Bundestag, Drucksache 16/12600, S. 78.

[242] *Rost/Meints*, Authentisierung in Sozialsystemen – Identitytheft strukturell betrachtet, DuD 2005, S. 218.

[243] *Busch*, Biometrie und Identitätsdiebstahl, DuD 2009, S. 317; Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 22. Tätigkeitsbericht, Deutscher Bundestag, Drucksache 16/12600, S. 78.

die missbräuchliche Nutzung von sensiblen persönlichen Daten wie Bankkontodaten oder Kreditkartennummern zu erheblichen finanziellen Schäden führen.

Aktuelle Relevanz – insbesondere durch das Web 2.0 – hat der Identitätsdiebstahl, also die Täuschung über die Identität einer Person, im Bereich der sozialen Netzwerke. Dort spielt er in erster Linie im Rahmen der sog. „Fake-User Accounts" eine gewichtige Rolle. Fake-User Accounts stellen Profilseiten von Nutzern auf sozialen Plattformen im Internet dar, mit denen reale Identitäten von Personen vorgetäuscht werden. Dritte treten so im Internet unter dem Namen eines anderen Mitglieds auf und verwenden dessen persönliche Daten zum Aufbau einer zweiten digitalen Persönlichkeit. Diese besondere Form des Identitätsdiebstahls wird auch als „Nicknapping" bezeichnet. Der Schaden ist in solchen Fällen weniger finanzieller als vielmehr immaterieller Art, da die betroffenen Personen u.a. durch Beschimpfungen und Belästigungen im eigenen Namen in Misskredit gebracht werden. Zudem werden die Opfer eines Identitätsdiebstahls durch das Zur-Schau-Stellen von kompromittierenden echten oder gefälschten Fotos, welche in das Mitgliederprofil integriert werden, bloß gestellt. Die Gefahr des Identitätsdiebstahls im Web 2.0 respektive im Bereich der sozialen Netzwerke liegt also in der Erstellung von realistischen Mitgliederprofilen.

## *III. Rechtliche Bewertung*

### *1. Allgemeines*

Hinsichtlich der strafbaren Handlungen kann zwischen dem Verschaffen und dem Verwenden der personenbezogenen Daten differenziert werden. Der Täter hat grundsätzlich zwei Möglichkeiten, an den Datensatz eines registrierten Mitgliedes zu gelangen.

Zum einen besteht die Möglichkeit, dass die Person sich in einem ersten Schritt selbst bei dem betreffenden Netzwerk registriert. Sodann kann sie auf alle innerhalb des Netzwerks öffentlich verfügbaren Informationen der Mitglieder zugreifen. Soweit diese freigegeben sind, gehören hierzu zum Beispiel der Name und die vollständige Anschrift, Geburtstag und –ort, Kontaktdaten, wie Handy- oder Telefonnummer und Instant Manager (Skype, ICQ).

Zum anderen stellen die Zugangsdaten, d.h. die E-Mail Adresse und das Passwort, das Einfallstor in die digitale Privatsphäre des Mitglieds eines sozialen Netzwerkes dar. Denn in der Regel loggen sich die Mitglieder mit Hilfe der registrierten E-Mail Adresse und eines frei gewählten Passwortes ein. Hier ist es allerdings unwahrscheinlich, dass die Zugangsdaten auf rechtswidrige Weise erlangt werden. Parallelen zum sog.

„Phishing“, welches im Identitätsdiebstahl auf wirtschaftlicher Seite, d.h. zum Beispiel im Bereich des Online-Banking, anzutreffen ist, können hier nicht gezogen werden. Beim Phishing versucht der Täter, den Empfänger durch eine E-Mail zu täuschen und zur Herausgabe von Zugangsdaten und Passwörtern für das Online-Banking auf einer hierzu eigens erstellten Internetseite, welche mit der Internetpräsenz der betreffenden Bank nahezu identisch ist, zu bewegen.[244] Im Bereich der sozialen Netzwerke, sind es jedoch meist einzelne Täter, die sich die Daten eines anderen Mitgliedes beschaffen. Vorgehensweisen wie das Phishing sind nicht denkbar, da hiermit ein zu hoher Aufwand verbunden wäre. Vielmehr ist es möglich, dass der Täter die Daten erlangt hat, weil das Opfer zum Beispiel ein ehemaliger Partner des Täters ist und er aufgrund gewisser Umstände innerhalb dieses Verhältnisses in den Besitz der Zugangsdaten gelangt ist. Somit ist grundsätzlich davon auszugehen, dass das Verschaffen der personenbezogenen Daten auf den Zugriff auf die innerhalb des Netzwerkes öffentlich verfügbaren Informationen registrierter Mitglieder beschränkt und in der Weise rechtlich nicht angreifbar ist.

Fraglich ist nun, wie sich die missbräuchliche Verwendung der personenbezogenen Daten rechtlich auswirkt. Konkret geht es darum, dass höchstpersönliche Informationen – und im Regelfall auch ein das Opfer darstellende Foto – eines Anderen in missbräuchlicher Weise für die Erstellung eines Mitgliederprofils in einem sozialen Netzwerk verwendet werden. Dabei soll die Betrachtung vorliegend bei den in diesem Zusammenhang wichtigsten Problemfeldern ihren Schwerpunkt finden.

### *2. Strafrecht*

Eine Strafbarkeit nach § 269 StGB wegen der Fälschung beweiserheblicher Daten ist vorliegend abzulehnen, da es am subjektiven Erfordernis der „Täuschung im Rechtsverkehr“ fehlt. Das Verwenden der Daten ist lediglich beschränkt auf die Darstellung der Profilpräsenz innerhalb des sozialen Netzwerks. Ein rechtlich erhebliches Verhalten seitens der betroffenen Person soll grundsätzlich nicht veranlasst werden.

Eine Strafbarkeit nach § 201a StGB wegen der Verletzung des höchstpersönlichen Lebensbereichs durch das Einstellen eines Foto, welches das Opfer erkennbar zeigt, liegt nicht vor. § 201a Abs. 3 StGB verlangt in diesem Zusammenhang, dass die Aufnahme eine Person zeigt, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet. Selbst wenn dieses Tatbestandsmerkmal bejaht werden kann, ist eine Strafbarkeit abzulehnen, da der Schutzweck der Norm ein ande-

[244] Vgl. zu diesen Ausführungen den Aufsatz von *Gercke*, Die Strafbarkeit von „Phishing“ und Identitätsdiebstahl, CR 2005, S. 606 ff.

rer ist. Geschützt werden soll der höchstpersönliche Lebensbereich vor Bildaufnahmen, welche das Opfer nachteilig beeinträchtigen.[245] Vorausgesetzt, der Dritte stellt ein sozialadäquates Foto[246] ein, wie es in sozialen Netzwerken üblich ist, liegt eine Verletzung der Intimsphäre nicht vor.

Fraglich ist des Weiteren, ob die missbräuchliche Verwendung personenbezogener Daten der betreffenden Person durch das Erstellen einer Profilseite in einem sozialen Netzwerk als eine Beleidigung aufzufassen ist. Möglich erscheint hier eine Strafbarkeit nach § 185 StGB. Als Beleidigung im Sinne des § 185 StGB ist die Kundgabe eigener Nichtachtung oder Missachtung zu verstehen.[247] Die Verwendung der Daten müsste dann als Kundgabe zu werten sein. Die Kundgabe erfolgt in den meisten Fällen als eine verbale mündliche Äußerung. Die lesbare schriftliche Fixierung tritt jedoch ergänzend hinzu.[248] Problematisch erscheint es allerdings, einen ehrenrührigen Inhalt in der schriftlichen Wiedergabe persönlicher Daten zu sehen, ohne eine Wertung dahinter erkennen zu können. Eine Äußerung ist beleidigend, wenn der objektiv ehrenrührige Sinn in der Erklärung einen erkennbaren Ausdruck gefunden hat.[249] Die Kundgabe muss ihrem objektiven Sinngehalt nach die Erklärung eines Mangels an Ehre zum Ausdruck bringen. Vorliegend würde es dennoch bei einer rein subjektiven Betrachtung bleiben, da nach der Intention des Täters gefragt werden müsste. Bei einer objektiven Betrachtung ist eine Erkennbarkeit des ehrenrührigen Sinngehalts vielmehr zu verneinen. Denn zu beachten bleibt, dass die Verletzung der Persönlichkeit zwar die Menschenwürde verletzt, zugleich aber nicht zwingend die Ehre tangiert.

Das Verwenden eines das Opfer darstellenden Fotos ist gleichfalls als eine Form der Kundgabe zu sehen[250] und kann den Tatbestand einer Beleidigung erfüllen. Voraussetzung hierzu ist es jedoch, dass das Opfer durch die Darstellung in aufreizender oder leichtbekleideter Pose in ehrenrühriger Weise gezeigt wird. Hierin käme ein nach außen wirkendes ehrverletzendes Werturteil zum Ausdruck. Dies ist jedoch im Einzelfall zu beurteilen, würde allerdings eine Strafbarkeit wegen Beleidigung nach § 185 BGB begründen.

---

[245] *Kindhäuser*, Lehr- und Praxiskommentar zum Strafgesetzbuch, 4. Auflage 2010, § 201a, Rdnr. 7.

[246] Anders liegt der Fall beispielsweise, wenn der Täter ein Nacktfoto – unerheblich, ob echt oder gefälscht – der betroffenen Person einstellt.

[247] *Kindhäuser*, Lehr- und Praxiskommentar zum Strafgesetzbuch, 4. Auflage 2010, § 185, Rdnr. 4.

[248] *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Leipziger Kommentar zum Strafgesetzbuch, Band VI (§§ 146-210), 12. Auflage 2010, § 185, Rdnr. 15.

[249] *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Leipziger Kommentar zum Strafgesetzbuch, Band VI (§§ 146-210), 12. Auflage 2010, § 185, Rdnr. 17.

[250] *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Leipziger Kommentar zum Strafgesetzbuch, Band VI (§§ 146-210), 12. Auflage 2010, § 185, Rdnr. 15.

Fraglich ist die strafrechtliche Bewertung der Fälle, in denen der Täter im Namen des Opfers einen Dritten beleidigt. Durch das erfolgreiche Erstellen eines Profils mithilfe fremder personenbezogener Daten ist der Täter in der Lage, innerhalb des sozialen Netzwerkes anderen registrierten Mitgliedern im Namen des Opfers Nachrichten zu schicken. So eröffnet sich ihm die Möglichkeit ehrenrührige Äußerungen gegenüber anderen Mitgliedern kund zu tun und diese folglich direkt zu beleidigen. Möglicherweise könnte sich somit das Opfer selbst wegen der Beleidigung strafbar machen. Hierzu ist auszuführen, dass „Täter" im Rahmen der Beleidigung nach § 185 BGB nur sein kann, wer vorsätzlich eigene Missachtung kundgibt.[251] Da das Opfer die Kundgabe ehrverletzender Äußerungen gar nicht beabsichtigt, ja nicht einmal von ihnen weiß, ist eine Strafbarkeit selbstredend abzulehnen. Bezüglich des Verwenders kann eine mittelbare Täterschaft in Betracht kommen, da er sich eines anderen, der vom Geschehen keine Kenntnis hat, zur Übermittlung der Äußerungen bedient.

### *3. Datenschutzrecht*

Fraglich ist, ob eine Strafbarkeit im Rahmen des Bundesdatenschutzgesetzes vorliegt. In Betracht kommt hier der Tatbestand des § 43 Abs. 2 Nr. 1 i.V.m. § 44 Abs. 1 BDSG. Danach wird unter anderem bestraft, wer vorsätzlich unbefugt personenbezogene Daten in der Absicht, einen anderen zu schädigen, erhebt oder verarbeitet. Durch ein Speichern der Daten auf dem Server des Netzwerkbetreibers erfüllt der Täter die Voraussetzungen. Allerdings ist der Tatbestand vorliegend dennoch abzulehnen, da das Bundesdatenschutzgesetz strafbegründend voraussetzt, dass auf nicht allgemein zugängliche Daten zugegriffen wird.[252] Wie bereits dargestellt wurde, sind die in die Verwendung der personenbezogenen Daten innerhalb des sozialen Netzwerks Eingang findenden Informationen – nach einer eigenen Registrierung – grundsätzlich, d.h. sofern der Täter keine näheren, aus anderen Quellen stammenden Informationen besitzt, allgemein zugänglich.

### *4. Kunsturhebergesetz*

Möglicherweise kommt aber das Kunsturhebergesetz zur Anwendung. Hintergrund für diese Überlegung ist, dass im Rahmen der missbräuchlichen Nutzung persönlicher Daten zur Erstellung eines realistischen Mitgliederprofils an das dazugehörige Einstel-

[251] *Fischer*, Kommentar zum Strafgesetzbuch, 57. Auflage 2010, § 185, Rdnr. 13; Rege, in: Münchener Kommentar zum Strafgesetzbuch, Band 3 (§§ 185-262), 2003, § 185, Rdnr. 39.

[252] *Dammann*, in: Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 6. Auflage 2006, § 43, Rdnr. 46.

len eines Bildes der betroffenen Person zu denken ist. Unterstellt, der Täter ist in den Besitz eines Fotos der betroffenen Person gelangt, ist fraglich, wie das Einstellen und Veröffentlichen dieses das Opfer darstellende Foto rechtlich zu behandeln ist. Das Kunsturhebergesetz (KUG) betrifft das Urheberrecht an Werken der bildenden Künste und der Fotografie und regelt zudem das Recht am Bildnis, d.h. an der äußeren Erscheinungsweise einer Person.[253]

In Frage kommt vorliegend eine Strafbarkeit nach § 22 i.V.m. § 33 Abs. 1 KUG wegen der Verletzung des Rechts am eigenen Bild. Nach § 22 KUG dürfen Bildnisse nur mit der Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Es handelt sich hierbei um den Schutz und die Normierung eines einzelnen Persönlichkeitsrechts. Von einer Einwilligung ist in Fällen des Identitätsdiebstahls im Bereich der sozialen Netzwerke grundsätzlich nicht auszugehen.

Ein Bildnis im Sinne des § 22 KUG ist gekennzeichnet durch jegliche Wiedergabe der äußeren Erscheinungsweise einer Person. Entscheidend ist lediglich die Erkennbarkeit des Abgebildeten. Es handelt sich also entsprechend dem Schutzzweck der Norm um die Abbildung einer Person, d.h. die Darstellung der Person in ihrer wirklichen, dem Leben entsprechenden Erscheinung.[254] Somit genügt hier das Einstellen eines Fotos, welches das Opfer erkennbar zeigt. Unerheblich ist, ob eine oder mehrere Personen abgebildet sind.[255] Vorliegend ist es somit ausreichend, falls die betreffende Person erkannt wird, sei es durch einen Bekannten oder durch jemanden aus dem Freundeskreis.[256] Sollten auf dem Foto neben dem Opfer weitere Personen zu sehen sein, spielt dies keine Rolle.

Unzulässig ist nach § 22 KUG die ungenehmigte Verbreitung sowie die öffentliche Zurschaustellung des Bildnisses. Vorliegend könnte die zweite Alternative, die öffentliche Zurschaustellung einschlägig sein. Zurschaustellen bedeutet, Dritten die Möglichkeit zu verschaffen, das Bildnis wahrzunehmen. Aufgrund der weiten Definition unterliegt somit auch das Einstellen von Fotos im Internet dem Anwendungsbereich des § 22 KUG.[257] An das Merkmal „öffentlich“ werden keine strengen Voraussetzungen ange-

---

[253] *Rehbinder*, Urheberrecht, 16. Auflage, 2010, S. 326, Rdnr. 856.

[254] *Dreier*, in: Dreier/Schulze (Hrsg.), Kommentar zum Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz und Kunsturhebergesetz, 3. Auflage 2008, § 22 KUG, Rdnr. 1.

[255] *Dreier*, in: Dreier/Schulze (Hrsg.), Kommentar zum Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz und Kunsturhebergesetz, 3. Auflage 2008, § 22 KUG, Rdnr. 1.

[256] Ist der Abgebildete auf die Veröffentlichung des Bildnisses angesprochen worden, z.B., weil die betroffene Person bereits ein Mitgliedskonto innerhalb des sozialen Netzwerks besitzt, so ist hierin die Bestätigung der Erkennbarkeit zu sehen. Vgl. hierzu *Dreier*, in: Dreier/Schulze (Hrsg.), Kommentar zum Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz und Kunsturhebergesetz, 3. Auflage 2008, § 22 KUG, Rdnr. 4.

[257] *Dreier*, in: Dreier/Schulze (Hrsg.), Kommentar zum Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz und Kunsturhebergesetz, 3. Auflage 2008, § 22 KUG, Rdnr. 11.

knüpft. Heranziehen lässt sich die Definition des § 15 Abs. 3 UrhG. Hiernach ist die Wiedergabe öffentlich, wenn sie für eine Mehrzahl von Mitgliedern der Öffentlichkeit bestimmt ist. Zur Öffentlichkeit gehört in diesem Zusammenhang jeder, der nicht mit demjenigen, der das Bildnis verwertet, oder mit den anderen Personen, denen das Bildnis wahrnehmbar oder zugänglich gemacht wird, durch persönliche Beziehungen verbunden ist. Folglich ist es ausreichend, wenn der Täter das Foto der betroffenen Person innerhalb des sozialen Netzwerkes öffentlich zugänglich macht. Indem er das Foto in die Profilpräsenz integriert, stellt der Täter das Foto öffentlich zur Schau.

Im Ergebnis verletzt der Täter somit § 22 KUG. Für den Fall der Zuwiderhandlung gegen § 22 KUG bestimmt die Vorschrift des § 33 Abs. 1 KUG eine Freiheitsstrafe bis zu einem Jahr oder die Zahlung einer Geldstrafe.

### *5. Grundgesetz*

Fraglich ist weiter, ob die missbräuchliche Verwendung der personenbezogenen Daten das Opfer in seinem allgemeinen Persönlichkeitsrecht beeinträchtigt[258]. Das allgemeine Persönlichkeitsrecht wird verstanden als das Recht des Einzelnen gegenüber jedermann auf Achtung seiner Menschenwürde und Entfaltung seiner individuellen Persönlichkeit.[259] Die Achtung der allgemeinen Persönlichkeit hat sich zu einem eigenen Grundrecht verselbstständigt und findet seinen normativen Bezugspunkt in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[260] Das geschützte Gut liegt in der engeren persönlichen Lebenssphäre und hierbei unter anderem in dem Verfügungsrecht über die Darstellung der eigenen Person.[261]

Möglicherweise ist das Opfer durch das unbefugte Erstellen eines Mitgliederprofils in seinem Verfügungsrecht bzgl. der Darstellung der eigenen Person verletzt. Geschützt ist der Einzelne jedoch nur gegen die verfälschende oder entstellende Darstellung seiner Person in der Öffentlichkeit, die von nicht ganz unerheblicher Bedeutung für die Persönlichkeitsentfaltung sein muss.[262] Der Identitätsmissbrauch durch das Erstellen eines Profils in einem sozialen Netzwerk ist hingegen nicht als verfälschend oder entstellend zu werten. Das Verwenden der Daten, die der Realität entsprechen, wird somit nicht erfasst.

---

[258] Siehe zum allgemeinen Persönlichkeitsrecht, dessen Verletzung und den Möglichkeiten der Sanktionierung den Aufsatz von *Hermann*, Caroline, Marlene und Lafontaine – Dimensionen des Persönlichkeitsrechtsschutzes, Life & Law 2010, S. 334 ff.

[259] *Teichmann*, in: Jauernig (Hrsg.), Kommentar zum Bürglichen Gesetzbuch, 13. Auflage 2009, § 823, Rdnr. 65.

[260] *Jarass*, in: Jarass/Pieroth, Kommentar zum Grundgesetz, 10. Auflage 2009, Art. 2, Rdnrn. 38 f.

[261] *Jarass*, in: Jarass/Pieroth, Kommentar zum Grundgesetz, 10. Auflage 2009, Art. 2, Rdnr. 41.

[262] *Jarass*, in: Jarass/Pieroth, Kommentar zum Grundgesetz, 10. Auflage 2009, Art. 2, Rdnr. 42.

Die Darstellung einer Person umfasst allerdings auch Verhaltensweisen und Äußerungen. Eine Folge des „Nicknapping“ sind in vielen Fällen Beschimpfungen und Belästigungen, die im Namen des Opfers abgegeben werden, um die betroffene Person zu diskreditieren. Hierbei werden der Person, in dessen Namen die Beleidigungen erfolgen, Äußerungen in den Mund gelegt, die sie nicht getan hat. Diese Beeinträchtigungen sind vom Schutz durch das allgemeine Persönlichkeitsrecht umfasst.[263]

Darüber hinaus erfasst das allgemeine Persönlichkeitsrecht zum einen den Schutz des Namens, sei es der Familienname oder der Vorname.[264] Zum anderen gewährleistet das Grundrecht als Recht auf informationelle Selbstbestimmung dem Einzelnen die Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmten. Somit wird das unbefugte Einstellen der personenbezogenen Daten durch einen Dritten vom Schutzbereich des allgemeinen Persönlichkeitsrechts erfasst. Die Befugnis der betroffenen Person über die Preisgabe persönlicher Lebenssachverhalte selbst entscheiden zu können, wird durch den Identitätsdiebstahl grundlegend tangiert.

Aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG folgt zudem das Recht am eigenen Bild als besonderes Persönlichkeitsrecht im Hinblick auf dessen Veröffentlichung sowie das Recht am eigenen Wort.[265] Letzteres wird beeinträchtigt, sobald der Täter im Namen des Opfers Textnachrichten jeglicher Art innerhalb des Netzwerkes verschickt. Die Sanktionierung der Verletzung des allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG wird aufgrund ihres zivilrechtlichen Charakters im nächsten Kapitel besprochen.

### *6. Bürgerliches Gesetzbuch*

Verwendet ein Dritter persönliche Daten des Opfers, um in einem sozialen Netzwerk eine Identität zu erstellen, ist an das Deliktsrecht, d.h. das Recht der unerlaubten Handlungen zu denken. Möglicherweise besteht hier eine Schadensersatzpflicht aus § 823 BGB. Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

Möglicherweise kommt hier die Verletzung eines sonstigen Rechts im Sinne des § 823 Abs. 1 BGB in Betracht. Sowohl das allgemeine Persönlichkeitsrecht, als auch das Recht am eigenen Bild als besondere Ausformung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sind als ein sonstiges Recht im Sinne

[263] *Jarass*, in: Jarass/Pieroth, Kommentar zum Grundgesetz, 10. Auflage 2009, Art. 2, Rdnr. 42.
[264] *Jarass*, in: Jarass/Pieroth, Kommentar zum Grundgesetz, 10. Auflage 2009, Art. 2, Rdnr. 43.
[265] *Jarass*, in: Jarass/Pieroth, Kommentar zum Grundgesetz, 10. Auflage 2009, Art. 2, Rdnr. 44.

des § 823 Abs. 1 BGB anerkannt.[266] Eine Verletzung ist grundsätzlich in jedem Verhalten zu sehen, welches dazu geeignet ist, eine nachteilige Beeinträchtigung der in Absatz 1 genannten Rechtsgüter herbeizuführen. Die hier gezeigte missbräuchliche Verwendung der persönlichen Informationen eines Anderen stellt eine Verletzung des allgemeinen Persönlichkeitsrechts sowie des Rechts am eigenen Bild dar. Ein sonstiges Recht wurde mithin verletzt.

Die Rechtswidrigkeit und das Verschulden in Form von Vorsatz können in den Fällen des Identitätsdiebstahls grundsätzlich als gegeben unterstellt werden. Eine Zuwiderhandlung gegen § 823 Abs. 1 BGB liegt somit vor. Die Rechtsprechung hat zur Sanktionierung der Verletzung des allgemeinen Persönlichkeitsrechts im Wege der richterlichen Rechtsfortbildung einen Sonderrechtsbehelf auf der Grundlage von § 823 Abs. 1 BGB i.V.m. dem Schutzauftrag aus Art. 2 Abs. 1, 1 Abs. 1 GG entwickelt, die sog. Geldentschädigung[267]. Somit besteht ein Anspruch auf Ersatz des entstandenen Schadens in Geld.

Gleichwohl könnte darüber hinaus ein Anspruch aus § 823 Abs. 2 BGB bestehen. Somit trifft die gleiche Schadensersatzpflicht denjenigen, „welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt“. Der Anwendungsbereich des Schutzgesetzes ist weit gefasst. Hierunter fallen jegliche Rechtsnormen, welche den Schutz eines Rechtsgutes sowie seines Inhabers bezwecken.[268] Sowohl das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als auch das Recht am eigenen Bild gemäß § 22 KUG stellen demnach ein Schutzgesetz im Sinne des § 823 Abs. 2 BGB dar. Die Pflicht zum Schadensersatz besteht auch hier.

Eine weitere Schadensersatzpflicht ergibt sich aus § 826 BGB aufgrund sittenwidriger vorsätzlicher Schädigung. Durch das öffentliche Zugänglichmachen der Daten des Opfers innerhalb des sozialen Netzwerks und der dadurch entstehenden Täuschung über ihre Identität verstößt der Täter in vorsätzlicher Weise gegen die guten Sitten. Grundsätzlich ist dieses Verhalten erheblich dazu geeignet, das Anstandsgefühl aller billig und gerecht denkenden Menschen in verletzender Weise zu tangieren.[269] Die Zufügung eines

---

[266] *Sprau*, in: Palandt (Begr.), Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage 2010, § 823, Rdnrn. 15, 19; *Dreier*, in: Dreier/Schulze (Hrsg.), Kommentar zum Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz und Kunsturhebergesetz, 3. Auflage 2008, §§ 33 ff. KUG, Rdnr. 2.

[267] *Hermann*, Caroline, Marlene und Lafontaine – Dimensionen des Persönlichkeitsrechtsschutzes, Life & Law 2010, S. 336.

[268] *Sprau*, in: Palandt (Begr.), Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage 2010, § 823, Rdnrn. 56a f.

[269] Vgl. hierzu *Sprau*, in: Palandt (Begr.), Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage 2010, § 826, Rdnr. 4.

(immateriellen) Schadens liegt hierbei in der Verletzung der Persönlichkeitssphäre der betroffenen Person.[270]

Über die genannten Schadensersatzansprüche hinaus stehen dem Opfer zudem Unterlassungs- und Beseitigungsansprüche zu. So gewährt § 1004 Abs. 1 S. 1 BGB in analoger Anwendung dem Opfer einen Anspruch auf Beseitigung der Verletzungshandlung.[271] Der Verwender ist nach der Geltendmachung dieses Anspruchs dazu verpflichtet, die Profilseite der betreffenden Person zu löschen. Sollte eine ernsthafte Wiederholungsgefahr bestehen, so besteht ein quasi-negatorischer Unterlassungsanspruch gemäß § 1004 Abs. 1 S. 2 BGB.

[270] Eine Schadensersatzpflicht begründet § 826 BGB nicht nur bei einer Beeinträchtigung der Vermögenslage, sondern darüberhinaus auch bei einer Verletzung ideeller Interessen oder der Persönlichkeitssphäre. Siehe hierzu *Teichmann*, in: Jauernig (Hrsg.), Kommentar zum Bürglichen Gesetzbuch, 13. Auflage 2009, § 826, Rdnr. 5.

[271] *Dreier*, in: Dreier/Schulze (Hrsg.), Kommentar zum Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz und Kunsturhebergesetz, 3. Auflage 2008, §§ 33 ff. KUG, Rdnrn. 2, 9 ff.; *Sprau*, in: Palandt (Begr.), Kommentar zum Bürgerlichen Gesetzbuch, 69. Auflage 2010, § 823, Rdnr. 123.

# Kapitel 4: Cyberterrorismus

*S. Röchner*

## *I. Einführung*

Der Begriff des Cyberterrorismus wurde erstmals von Barry C. Collin in den 1980er Jahren geprägt.[272] Was jedoch genau unter Cyberterrorismus zu verstehen ist, ist bis heute strittig. Obwohl weltweit über das Phänomen des Cyberterrorismus diskutiert wird und es bereits viele Stimmen in der Literatur hierzu gibt, konnte noch keine allgemein anerkannte Begriffsbestimmung gefunden werden. Ein Grund hierfür liegt in der Tatsache, dass bereits die Termini „Cyberspace" und vor allem „Terrorismus", die die Grundsteine des Cyberterrorismus bilden, noch nicht allgemeingültig definiert sind.[273] Zudem divergieren die Meinungen, wie weit der Begriff des Cyberterrorismus gefasst werden muss, sehr.[274] Diese unterschiedlichen Sichtweisen führen dazu, dass auch die Ansichten darüber, wie groß die Gefahr vor einem cyberterroristischen Anschlag tatsächlich ist, weit auseinander gehen.[275] Trotzdem ist es wichtig, eine einheitliche Begriffsbestimmung zu finden. Nur wenn bekannt ist, was Cyberterrorismus tatsächlich bedeutet und wie groß die Gefahr einer cyberterroristischen Tat ist, können wirksame Rechtsgrundlagen zu seiner Bekämpfung geschaffen werden.[276]

## *II. Der Begriff des Cyberterrorismus*

### *1. Cyberspace und Terrorismus*

Der Begriff des Cyberterrorismus setzt sich zusammen aus den zwei Wörtern „Cyberspace" und „Terrorismus" und beschreibt die Konvergenz zwischen diesen beiden Bereichen.[277] Daher ist es sinnvoll sich mit diesen Termini zu befassen, bevor auf den Cyberterrorismus selbst eingegangen wird.

Cyberspace kann definiert werden als virtuelle Welt, als Ort des Datenverkehrs[278], und wird heute im allgemeinen Sprachgebrauch mit dem Internet gleichgesetzt[279]. Diese Begriffsbestimmung wird den folgenden Ausführungen zugrunde gelegt.

---

[272] *Collin,* The Future of CyberTerrorism, http://afgen.com/terrorism1.html (Stand: 25.05.2010).
[273] Weitere Ausführungen hierzu unter II. 1.
[274] Weitere Ausführungen hierzu unter II. 2.
[275] Weitere Ausführungen hierzu unter V.
[276] So auch *Bubnhoff*, NJW 2002, 2672 in Bezug auf den traditionellen Terrorismus.
[277] *Denning*, Cyberterrorism, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Stand: 25.05.2010).
[278] *Collin,* The Future of CyberTerrorism, http://afgen.com/terrorism1.html (Stand: 25.05.2010).
[279] *Fischer*, www.InfrastrukturInternet-Cyberterror.Netzwerk, 2007, S. 122.

Problematischer ist die Definition des Terrorismus. Bis heute gibt es keine Definition, die international Anerkennung gefunden hat.[280] Innerhalb der Europäischen Union wurden mit dem Rahmenbeschluss des Rates zur Terrorismusbekämpfung vom 13. Juni 2002 die Definitionen terroristischer Straftaten angeglichen.[281] Nach Art. 1 I des Rahmenbeschlusses liegt eine terroristische Straftat dann vor, wenn bestimmte, vorsätzlich begangene Straftaten durch die Art ihrer Begehung oder ihren jeweiligen Kontext ein Land oder eine internationale Organisation ernsthaft schädigen können, und mit dem Ziel begangen werden, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation rechtswidrig zu einem Tun oder Unterlassen zu zwingen, oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Landes oder einer internationalen Organisation ernsthaft zu destabilisieren oder zu zerstören. Art 1 I enthält auch eine Aufzählung der Straftaten, die unter den gerade genannten Voraussetzungen als terroristische Taten eingestuft werden können. Dabei handelt es sich vor allem um schwerwiegende Taten. Dazu gehören unter anderem Angriffe auf das Leben oder die körperliche Unversehrtheit eines Menschen, die Zerstörung öffentlicher Einrichtungen, Verkehrsmittel oder Infrastrukturen einschließlich Informatiksystemen, sowie das Kapern öffentlicher Verkehrsmittel und die Zerstörung oder Unterbrechung der Versorgung mit lebenswichtigen natürlichen Ressourcen wie Wasser oder Strom. Auch die reine Drohung mit der Begehung solcher Taten kann eine terroristische Tat darstellen. Nach der Definition des Rahmenbeschlusses charakterisieren also folgende Merkmale den Terrorismus:

- Begehung bestimmter Straftaten bzw. Drohung mit solchen Taten
- Herbeiführung ernsthafter Schäden
- Politisch motivierte Zielsetzung: Einschüchterung der Bevölkerung, Zwangausübung auf ein Land oder Destabilisierung der Grundstrukturen.

Diese Elemente gelten auch in Deutschland als solche des Terrorismus, da hier die Vorgaben des Rahmenbeschlusses in § 129a StGB umgesetzt wurden. Bei einer Untersuchung verschiedener Definitionen des Terrorismusbegriffs lässt sich zudem feststellen, dass die Kennzeichen des Terrorismus, die sich aus den Vorgaben des Rahmenbeschlusses ergeben, in vergleichbarer Form in vielen der Definitionen zu finden sind.[282] Ein solches Ergebnis zeigt, dass eine Einigung über die exakte Begriffsbestimmung

[280] Grabitz/Hilf/*Röben*, Das Recht der Europäischen Union, Losebl. (Stand: Juli 2008), Art. 29 EUV Rn. 20.

[281] Rahmenbeschluss des Rates 2002/475/JI, ABl. 2002 L 164, Erwägungsgrund 6.

[282] So bestimmte Kerr nach einer Untersuchung von 109 akademischen und offiziellen Terrorismusdefinitionen folgende drei allgemeinen Merkmale: Gebrauch von Gewalt, politische Motivation und die Absicht, Angst in einer bestimmten Bevölkerung zu verbreiten, *Kerr*, Putting cyberterrorism into context http://www.auscert.org.au/render.html?it=3552 (Stand: 25.05.2010).

zwar noch nicht gelungen ist, bestimmte Elemente, die den traditionellen Terrorismus charakterisieren, jedoch überwiegend anerkannt sind. Da der Terrorismus ein Grundelement des Cyberterrorismus ist, sollten sich diese Merkmale des Terrorismus auch in der Definition des Cyberterrorismus finden.[283]

### *2. Weiter und enger Begriff des Cyberterrorismus*

Cyberterrorismus beschreibt ganz allgemein die Konvergenz zwischen Cyberspace und Terrorismus, also das Zusammentreffen von Terrorismus und der virtuellen Welt. Daher müssen im Rahmen eines cyberterroristischen Aktes Terroristen in irgendeiner Form im oder mittels des Internets handeln. Hier stellt sich zunächst die Frage, in welcher Weise Terroristen das Internet für ihre Zwecke nutzen können. Danach ist zu klären, ob jede Form der Nutzung auch als Cyberterrorismus gelten sollte.

#### *a) Nutzung des Internets durch Terroristen*

Terroristen können auf vielfältige Weise im und mittels des Internets tätig werden. Dabei ist die Unterscheidung verschiedener Formen des Handelns möglich. Zum einen können Terroristen das Internet als Logistikmittel nutzen, um ihre Ziele zu verfolgen, zum anderen kann das Internet auch selbst Ziel und Angriffsmittel sein.[284]

##### *aa) Das Internet als Logistikmittel*

Stellt das Internet für Terroristen ein logistisches Mittel dar, so wird es nicht als Ziel oder Mittel für die direkte Ausführung eines Anschlags eingesetzt, sondern dient vielmehr als Hilfsmittel für die logistischen Aufgaben innerhalb einer Vereinigung. Eine erste Möglichkeit das Internet als Logistikmittel zu nutzen, besteht in der Verbreitung von Propaganda.[285] Terroristische Gruppen können ihre eigenen Webseiten betreiben und so ihre Ansichten einem breiten Publikum öffentlich machen. Hier werden die verfolgten Ziele beschrieben und angewandte Mittel gerechtfertigt. Auch können Gegner in ein schlechtes Licht gerückt werden, um ein größeres Verständnis der eigenen Handlungen zu erreichen. Eng verknüpft mit dem Propagieren der eigenen Ziele ist die Rekrutierung neuer Mitglieder. So besteht die Möglichkeit auf Propagandaseiten im Internet Foren oder Chat-Rooms bereit zu stellen, in denen interessierte Personen Meinungen austauschen können. So können Personen, die die Ziele der terroristischen Organisation befürworten, kontaktiert und zu einer Mitarbeit bei Terroranschlägen motiviert werden. All dies kann durch die Einbindung multimedialer Elemente, die im Internet zur Verfü-

---

[283] So auch *Kerr*, Putting cyberterrorism into context, http://www.auscert.org.au/render.html?it=3552 (Stand: 25.05.2010).

[284] *Helfer*, Sicherheitspolitik 2006, Nr. 3 (Mai), S. 24; *Fischer*, www.InfrastrukturInternet-Cyberterror.Netzwerk, 2007, S. 90.

[285] Dazu: *Weimann*, www.terror.net, http://www.usip.org/files/resources/sr116.pdf (Stand: 25.05.2010), S. 6*; Gercke*, CR 2007, 62 (63f).

gung stehen, eindringlich vermittelt werden. So können Terroristen den virtuellen Raum in vielfältiger Weise zu Propagandazwecken nutzen.[286]

Daneben bietet sich das Internet auch zur Beschaffung finanzieller Mittel an.[287] Auf Internetseiten können Spendenaufrufe veröffentlicht und Daten von Bankkonten zur Überweisung von Spenden bekannt gemacht werden. Ebenso können Terroristen auf Webseiten ihren Befürwortern die Möglichkeit bieten, mittels einer Kreditkarte und einer Einzugsermächtigung direkt Geld zu spenden. Denkbar ist auch, dass mit dem Verkauf von DVDs, CDs, Büchern, Fahnen und Ähnlichem Geld eingenommen wird. Daher kann das Internet zur Finanzierung einer terroristischen Organisation herangezogen werden.[288]

Terroristen können das Internet auch zur Planung von Anschlägen nutzen.[289] Im Cyberspace findet sich eine Vielzahl von Informationen, die zum Gelingen von terroristischen Taten notwendig sind. So können unter anderem Daten über etwaige Terrorziele gesammelt werden. Beispielsweise lassen sich detaillierte Satellitenfotos von den meisten Orten der Welt finden oder bauliche Pläne militärischer Einrichtungen.[290] Daneben bietet das Internet Hilfe bei der Herstellung der Mittel, mit denen ein Anschlag verübt werden kann. Anleitungen zum Bau von Sprengsätzen können genauso dem World Wide Web entnommen werden, wie Informationen über Chemikalien, Bakterien oder Viren, mit deren Hilfe terroristische Angriffe denkbar sind.

Eine weitere Art der Internetnutzung durch Terroristen stellt die Kommunikation dar.[291] Mithilfe von E-Mails, Chats und Foren können Terroristen, die einer einzigen Organisation angehören, in Kontakt treten und notwendige Informationen austauschen. Aber auch den unterschiedlichen Gruppen wird die Kontaktaufnahme untereinander durch Chats oder Foren erleichtert. Die Kommunikation spielt auch im Rahmen der Planung von terroristischen Anschlägen eine Rolle. Nur wenn eine gute Verteilung und Koordinierung der für einen Angriff notwendigen Arbeiten gesichert ist, können Terroristen ihre Ziele erreichen. Mithilfe des Internets wird ihnen dies erheblich erleichtert.

---

[286] Eine beispielhafte Aufzählung darüber, welche Organisationen eigene Internetauftritte unterhalten findet sich bei: *Weimann*, www.terror.net, http://www.usip.org/files/resources/sr116.pdf (Stand: 25.05.2010), S. 3.

[287] Hierzu: *Furnell/Warren*, in O`Day: Cyberterrorism, 2004, S. 113; *Sieber/Brunst,* in: Council of Europe [Hrsg.], Cyberterrorism – the use of the Internet for terrorist purposes, 2007, S. 38.

[288] Beispiele zu terroristischen Vereinigungen, die das Internet zur Beschaffung finanzieller Mittel nutzen finden sich bei: *Weimann*, www.terror.net, http://www.usip.org/files/resources/sr116.pdf (Stand: 25.05.2010), S. 7f.

[289] *Fischer,* www.InfrastrukturInternet-Cyberterror.Netzwerk, 2007, S.129ff.

[290] *Gercke*, CR 2007, 62 (64).

[291] Vgl. *Weimann*, www.terror.net, http://www.usip.org/files/resources/sr116.pdf (Stand: 25.05.2010), S. 9.

Bei all den eben aufgeführten Tätigkeiten nutzen die Terroristen das Internet. Cyberspace und Terrorismus treffen also aufeinander. Es könnte sich hier demnach um cyberterroristische Taten handeln.[292]

*bb) Das Internet als Ziel und Angriffsmittel des Terrorismus*

Terroristen können das Internet nicht nur als logistisches Hilfsmittel bei der Ausführung physischer Angriffe nutzen. Vielmehr kann der Cyberspace auch selbst Ziel und Waffe des Terrorismus werden. So kann durch Hacker- oder DoS-Angriffe die Funktionstüchtigkeit des Internets selbst erheblich beeinträchtigt werden oder die Infrastruktur Internet durch die Zerstörung von Rechenzentren oder Glasfaserkabeln mittels Bomben- oder Brandanschläge physisch beschädigt werden. Dadurch wird das Internet selbst zur Zielscheibe von Terroristen.

Mittels Internet können aber auch mit diesem verbundene weitere Netzwerke und Infrastrukturen, insbesondere sogenannte kritische Infrastrukturen, angegriffen werden. Kritische Infrastrukturen sind die Elemente der Infrastruktur eines Landes, die von so großer Bedeutung sind, dass die Funktionsfähigkeit des Staates ohne sie erheblich gefährdet wird oder die Bevölkerung bei ihrem Ausfall einen erheblichen Wohlstandsverlust hinnehmen muss.[293] Beispiele hierfür sind das Bank- und Finanzwesen, das Verkehrswesen, das Telekommunikations-, Wasser- Strom- oder Gasnetz.[294] Viele dieser Infrastrukturen sind mit dem Internet verbunden.[295] So ist es möglich, online in die Computersysteme dieser Objekte einzudringen und auf diesem Weg die Systeme zu manipulieren oder auch zu beschädigen. Die Beeinträchtigung der betroffenen kritischen Infrastruktur könnte zu massiven Schädigungen des Staates führen, oder auch das Leben oder die Gesundheit von Menschen gefährden.[296] Durch Angriffe über das Internet können also auch Objekte und Personen in der realen Welt erreicht und Ziele von Anschlägen werden. So wird das Internet zum Angriffsmittel für Terroristen.

*b) Umfang des Cyberterrorismusbegriffs*

Bei all den verschiedenen Möglichkeiten, die sich Terroristen bieten, im und mittels des Internets zu handeln, stellt sich die Frage, ob all diese Arten der Ausnutzung des Cyberspace auch unter den Begriff des Cyberterrorismus zu fassen sind. In der Literatur lassen sich drei Definitionsansätze zur Begriffsbestimmung von „Cyberterrorismus“

[292] Siehe hierzu Ausführungen unter b).

[293] *Kuhn*, Der Schutz kritischer Infrasturkuren, http://www.ifsh.de/IFAR/pdf/wp5.pdf (Stand: 25.05.2010), S. 4.

[294] *Gercke*, CR 2007, 62 (65).

[295] *Sierber/Brunst*, in: Council of Europe [Hrsg.], Cyberterrorism – the use of the Internet for terrorist purposes, 2007, S. 17.

[296] Zu möglichen Angriffsszenarien siehe III.

unterscheiden.[297] Zunächst besteht die Möglichkeit, eine Definition des traditionellen Terrorismus an das Medium des Internets anzupassen. In einem zweiten Ansatz wird anhand bestehender Gesetze und Rechtsprechungen herausgearbeitet, welche Handlungen einen cyberterroristischen Akt begründen. Der dritte Definitionsansatz besteht darin, bereits bestehende Definitionsversuche mit spezifischen Handlungen zu verbinden und so eine Art Typologie des Cyberterrorismus zu entwickeln.

Unabhängig von dem jeweiligen Ansatz der Begriffsfindung lassen sich die entwickelten Definitionen anhand ihres Anwendungsbereichs unterscheiden. So wird der Terminus des Cyberterrorismus teilweise weit und teilweise eng gefasst. Nach einem Teil der Literatur soll jede Art der Nutzung des Internets durch Terroristen vom Begriff des Cyberterrorismus erfasst werden.[298] Begründet wird diese weite Begriffsbestimmung mit der Konvergenz von Cyberspace und Terrorismus, die den Cyberterrorismus charakterisiert. Eine solche Konvergenz sei nicht nur bei Angriffen auf oder mittels des Internets realisiert, sondern auch dann, wenn andere Möglichkeiten der virtuellen Welt eingesetzt werden, wenn also das Internet als logistisches Hilfsmittel zur Ausführung physischer Angriffe dient[299], beispielsweise bei der Kommunikation der Mitglieder einer terroristischen Gruppe.

Im Gegensatz dazu ist in der Literatur auch eine Reihe von Definitionen verbreitet, die den Umfang des Cyberterrorismusbegriffs im Vergleich zur weiten Begriffsbestimmung einschränken. Nach diesen umfasst der Cyberterrorismus nur rechtswidrige Angriffe oder Drohungen mit solchen, die auf das Internet und mittels des Internets ausgeübt werden.[300] Nutzungen des Internets als reines Logistikmittel gelten nach diesen Definitionen dagegen nicht als Cyberterrorismus. Strittig innerhalb dieser Ansicht ist wiederum, ob auch Anschläge auf das Internet, die mit physischen Mittel durchgeführt werden, wie die Zerstörung von Rechenzentren durch Bomben, zum Cyberterrorismus zu zählen sind.[301] Wird dies verneint, so führen einzig mittels Computer und Internet durchgeführte Anschläge auf den Cyberspace selbst oder auf eine ihm angeschlossene Infrastruktur zu einer cyberterroristischen Tat.

---

[297] Siehe hierzu: *Ballard/Hornik/McKenzie*, in: O`Day: Cyberterrorism, 2004, S. 42f.

[298] *Gordon/Ford*, in: O`Day, Cyberterrorism, 2004, S. 126; *Helfer*, Sicherheitspolitik 2006, Nr. 3 (Mai), S. 24; *Gercke*, CR 2007, 62 (63).

[299] *Gordon/Ford*, in: O`Day, Cyberterrorism, 2004, S. 126.

[300] *Denning*, Cyberterrorism, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Stand: 25.05.2010); *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 4; *Fischer*, www.InfrastrukturInternet-Cyberterror.Netzwerk, 2007, S. 90/174; *Kerr*, Putting cyberterrorism into context, http://www.auscert.org.au/render.html?it=3552 (Stand: 25.05.2010); *Conway*, Terrorism and IT, http://doras.dcu.ie/502/1/terrorism_it_2003.pdf (Stand: 25.05.2010), S. 5f.

[301] Bejahend, Fischer, www.InfrastrukturInternet-Cyberterror.Netzwerk, 2007, S. 90, verneinend, *Kerr*, Putting cyberterrorism into context, http://www.auscert.org.au/render.html?it=3552 (Stand: 25.05.2010).

Problematisch an einer weiten Ausdehnung des Cyberterrorismusbegriffs, die auch die Nutzung des Internets als Logistikmittel umfasst, ist, dass der terroristische Aspekt gering gewertet wird. Wie bereits gezeigt, können trotz fehlender allgemein anerkannter Definition bestimmte Merkmale des Terrorismus identifiziert werden. Dazu gehören die Schädigung eines Landes und die politisch motivierte Zielsetzung. Diese Merkmale finden im Rahmen einer weiten Definition des Cyberterrorismus zu wenig Beachtung. Nutzen Terroristen das Internet nämlich als logistisches Hilfsmittel zur Ausführung physischer Angriffe, so werden erst durch den Angriff selbst die genannten Elemente des Terrorismus verwirklicht, nicht jedoch durch die bloßen Handlungen im Cyberspace. Durch die Planung oder Kommunikation mittels Internet beispielsweise entstehen weder ernsthafte Schäden in einem Staat noch wird die Bevölkerung eingeschüchtert oder der Staat zu etwas gezwungen. Vielmehr handelt es sich um Taten im Vorfeld eines terroristischen Anschlags. Erst ein konkreter Angriff auf ein bestimmtes Ziel weist die Merkmale des Terrorismus auf. Aus diesem Grund sollte der Begriff des Cyberterrorismus nicht so weit verstanden werden, dass er jegliche Internetnutzung erfasst. Vielmehr sollte eine cyberterroristische Tat nur dann angenommen werden, wenn das Internet selbst das Ziel eines Angriffs ist, oder es als Angriffsmittel auf mit dem Internet verbundene kritische Infrastrukturen herangezogen wird.[302]

Dabei sollten jedoch physische Angriffe auf das Internet, beispielsweise durch die Inbrandsetzung wesentlicher Knotenpunkte, aus der Definition ausgenommen werden. Zwar besteht auch hier eine Verbindung zwischen Terrorismus und Cyberspace, diese liegt jedoch lediglich darin, dass das Ziel eines in traditioneller Form ausgeführten Angriffs, das Internet ist. Ein Unterschied zu anderen mit physischen Mitteln verwirklichten Terroranschlägen beispielsweise auf ein Gebäude, ergibt sich hierbei nicht. Vor allem werden keine Besonderheiten des Internets ausgenutzt. Es erscheint daher wenig sinnvoll, einen physischen Anschlag auf ein Gebäude als traditionellen Terrorismus, einen physischen Angriff auf das Internet jedoch als Cyberterrorismus zu qualifizieren. Daher sollte ein physischer Angriff auf das Internet nicht unter den Begriff des Cyberterrorismus gefasst werden.[303]

---

[302] Im Ergebnis ebenso: *Denning*, Cyberterrorism, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Stand: 25.05.2010); *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 4; *Kerr*, Putting cyberterrorism into context, http://www.auscert.org.au/render.html?it=3552 (Stand: 25.05.2010); *Conway*, Terrorism and IT, http://doras.dcu.ie/502/1/terrorism_it_2003.pdf (Stand: 25.05.2010), S. 5f.

[303] Ebenso: *Kerr*, Putting cyberterrorism into context, http://www.auscert.org.au/render.html?it=3552 (Stand: 25.05.2010).

### *3. Zwischenergebnis*

Es kann also festgehalten werden, dass Cyberterrorismus bestimmte Merkmale, die den Terrorismus kennzeichnen, erfüllen muss. Dabei handelt es sich um die Verwirklichung von Straftaten oder die Drohung mit solchen, die Herbeiführung ernsthafter Schäden und eine politisch motivierte Zielsetzung. Zudem sind Angriffe, die mittels des Internets auf das Internet selbst oder auf mit diesem verbundene Infrastrukturen ausgeübt werden, unter Cyberterrorismus zu fassen, nicht jedoch die Nutzung des Internets als Logistikmittel. Fasst man diese gewonnenen Erkenntnisse zusammen, kann Cyberterrorismus als ein rechtswidriger Angriff in Form einer Manipulation oder Schädigung, oder die Androhung eines solchen, auf das Internet oder auf mit dem Internet verbundene Netzwerke und Infrastrukturen, der mittels Computer und Internet ausgeübt wird, eine politisch motivierte Zielsetzung und ernsthafte Schäden zur Folge hat, beschrieben werden. Diese Definition des Cyberterrorismus wird dem Folgenden zugrunde gelegt.

### *4. Abgrenzung zum Cybercrime und zum Hacktivismus*

Nicht verwechselt werden darf der Cyberterrorismus mit Cybercrime oder Hacktivismus. Cybercrime und Cyberterrorismus sind keine austauschbaren Begriffe. Vielmehr bildet Cybercrime gewissermaßen einen Oberbegriff, der auch den Cyberterrorismus erfasst. Unter Cybercrime sind ausgehend von der Begriffsbestimmung des Europarates in der Convention on Cybercrime[304] jede illegale Aktivitäten zu verstehen, die mittels Computer in Verbindung mit einem elektronischen Netzwerk begangen werden.[305] Ein Fall des Cybercrime ist der Cyberterrorismus, bei dem die illegale Aktivität im politisch motivierten Angreifen des Internets oder einer mit diesem verbundenen Infrastruktur liegt, und ernsthafte Schäden des betroffenen Staates herbeiführt.

Abzugrenzen ist der Cyberterrorismus auch vom sogenannten Hacktivismus. Hacktivismus beschreibt die Verbindung von Hacking mit politischem Aktivismus.[306] Dabei wird unter Hacking das Eindringen in ein fremdes Computersystem über ein Netzwerk verstanden.[307] Hacktivisten greifen damit ebenso wie Cyberterroristen aus politischen Motiven Computer über das Internet an. Im Unterschied zu diesen wollen sie jedoch keine ernsthaften Schäden anrichten oder gar Menschen verletzen, sondern vielmehr

[304] ETS Nr. 185.

[305] *Laue*, jurisPR-StrafR 13/2009, Anm. 2, S. 3.

[306] *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 4.

[307] Erreicht wird hierdurch der bloße Zugang zu den Daten im System, ein Abrufen der Daten ist nicht erforderlich; BT-Drs. 16/3656, S. 9.

einen gewaltlosen Protest gegen etwas ausdrücken.[308] Dadurch unterscheidet sich der Hacktivismus vom Cyberterrorismus und darf nicht mit diesem verwechselt werden.

### *III. Hypothetische Angriffsszenarien*

Nachdem bisher der Begriff des Cyberterrorismus abstrakt dargestellt wurde, sollen nun beispielhaft konkrete Szenarien gezeigt werden, wie ein cyberterroristischer Anschlag aussehen könnte.[309] Da bisher kein Fall bekannt geworden ist[310], der unter die hier vertretene Definition des Cyberterrors gefasst werden kann, handelt es sich hierbei um rein hypothetische Angriffszenarien. Ob diese in der Praxis tatsächlich umsetzbar wären und die gewünschten Folgen herbeiführen würden, bleibt bei dieser Betrachtung unberücksichtigt.

Beispiel 1: Ein erstes mögliches Szenario besteht in einem Angriff von Terroristen auf die Computersysteme der medizinischen Industrie. Sie dringen in das System eines Pharmaunternehmens ein und manipulieren die computergesteuerte Zusammensetzung der Medikamente, so dass diese lebensgefährliche Auswirkungen auf Patienten haben.

Beispiel 2: Im zweiten Fall dringen die Täter in das Netzwerk eines Lebensmittelherstellers ein und manipulieren die Zusammensetzung von Lebensmitteln in der Weise, dass sie nun in großen Mengen gefährliche Bestandteile enthalten. Die Folgen könnten hier mit denen des sogenannten Milchpulverskandals in China aus dem Jahre 2008 vergleichbar sein. Dort enthielt ein für die Zubereitung von Säuglingsnahrung vorgesehenes Milchpulver die Chemikalie Melamin, wodurch viele Babys, die die betroffene Nahrung verzehrten, schwer erkrankten und einige Kinder starben. Hieran zeigt sich, welche schwerwiegenden Folgen eine falsche Zusammensetzung von Lebensmitteln haben kann.

Beispiel 3: Denkbar ist weiterhin, dass Terroristen einen Angriff auf Computersysteme der Flugverkehrsüberwachung ausüben. In einem solchen Fall könnten sie die Steuerung von Flugzeugen mittels des Computers übernehmen und die Kollision zweier Passagierflugzeuge herbeiführen. Der Tod vieler Menschen wäre die Folge.

Beispiel 4: Ein weiteres Szenario stellt der Angriff auf das Netzwerk eines Kernkraftwerkes dar. Die Terroristen könnten mit dem Computer den Ablauf oder Kontrollmechanismen des Kraftwerks manipulieren und so eine Explosion durch Kernenergie auslösen.

---

[308] *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 5.

[309] Vgl. hierzu *Collin*, The Future of CyberTerrorism, http://afgen.com/terrorism1.html (Stand: 25.05.2010).

[310] *Sieber/Brunst*, in: Council of Europe [Hrsg.], Cyberterrorism – the use of the Internet for terrorist purposes, 2007, S. 16.

Beispiel 5: Auch ein Angriff auf das Computersystem einer Staumauer ist denkbar. Nachdem die Täter in das System eingedrungen sind, öffnen sie die computergesteuerten Tore. Durch die folgende Überschwemmung wird das Leben all jener Menschen gefährdet, die sich im betroffenen Gebiet befinden.

### *IV. Vorteile des Internets*

Der folgende Abschnitt widmet sich der Frage, warum Terroristen überhaupt das Internet als Angriffsmittel nutzen könnten, anstatt ihre Ziele weiterhin mit traditionellen Mitteln zu verfolgen. Die Ausführung von Anschlägen via Internet ist in vielerlei Hinsicht vorteilhaft für Terroristen.[311] Die Verbreitung des Internets nimmt immer weiter zu. In vielen Lebensbereichen werden Computersysteme eingesetzt, die in den meisten Fällen auch miteinander vernetzt werden. Dadurch entsteht eine große Vielfalt potentieller Ziele, die alle für Terroristen über das Internet erreichbar sind. Ein weiterer Vorteil ist, dass die physische Anwesenheit des Attentäters am Ort des Anschlags nicht nötig ist. Vielmehr kann der Täter seinen Angriff von irgendeinem Ort auf der Welt durchführen. Die Gefahr einer Verletzung oder gar Tötung des handelnden Terroristen selbst entfällt hierdurch. Daneben kann auch die Gefahr, dass der Täter nach der Tat oder gar schon im Vorfeld des Anschlags gefasst und bestraft wird, durch den Einsatz des Internets verringert werden. Dies lässt sich auf die Anonymität zurückführen, die die vernetzte Welt mit sich bringt. In den Cyberspace gelangt man mit einem beliebigen Zugang. Es ist nicht notwendig eine private Verbindung zu nutzen, sondern es besteht die Möglichkeit anonym nutzbare Zugänge, wie sie beispielsweise in Internetcafés angeboten werden, zu verwenden. Im Netz selbst kann ohne Angabe der eigenen Identität, falls nötig unter Heranziehung eines fiktiven Benutzernamens oder einer Gastkennung, verkehrt werden. Diese Anonymität erschwert die Chance, einen Täter zu fassen erheblich. Zudem sind bei weltweiten Aktivitäten die Behörden verschiedener Länder in die Bekämpfung des Terrorismus involviert. Die notwendige Koordination der betroffenen Stellen ist aufgrund fehlender gemeinsamer Handlungsrichtlinien oft kompliziert und langwierig.[312] Ein weiterer Vorteil der Instrumentalisierung des Internets besteht darin, dass die Kosten für einen Anschlag billiger sind, als bei einem traditionellen Anschlag.[313] Terroristen müssen keine Waffen oder Sprengstoff kaufen, sondern benötigen lediglich einen Computer und eine Internetanbindung. Darin liegt ein weiterer Vorzug, der die Ausführung eines Anschlags mittels Internet für Terroristen interessant machen kann.

---

311 Zum Folgenden vgl.: *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 6.

312 *Gercke*, CR 2007, 62 (68f).

313 *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 6.

### *V. Gefahr eines cyberterroristischen Anschlags*

Bei all diesen Vorteilen, die das Internet bietet, drängt sich die Frage auf, wie groß die Gefahr, dass ein cyberterroristischer Anschlag verübt wird, tatsächlich ist. Müssen Staaten jederzeit mit einem solchen Angriff rechnen oder ist die Angst davor übertrieben? In der Literatur ist dies neben der Problematik der Begriffsbestimmung ein lebhaft diskutiertes Thema des Cyberterrorismus. Die Meinungen dazu gehen weit auseinander. So wird einerseits die Ansicht vertreten, dass Cyberterrorismus ein Mythos ist.[314] Es gebe keine Hinweise darauf, dass Terroristen Anschläge im Cyberspace planen, mit denen sie die gleichen verheerenden Folgen erzielen wollen, wie bei physischen Anschlägen. Durch die Diskussion über den Cyberterror könne es passieren, dass die dringendere Gefahr vor physischen Terroranschlägen in den Hintergrund gerückt werde. Ganz im Gegensatz hierzu wird auch die Ansicht vertreten, dass Cyberterrorismus eine ernstzunehmende akute Gefahr darstellt, die nicht zu unterschätzen ist.[315] Vor allem in den Massenmedien wird immer wieder vor Anschlägen gewarnt oder über angeblichen Cyberterror berichtet.[316]

Gründe für diese erheblichen Abweichungen bei der Einschätzung der Terrorgefahr liegen unter anderem im Interesse der Massenmedien an diesem Thema und in der Definitionsvielfalt. Die Medien haben den Cyberterrorismus längst als umsatzsteigernde Schlagzeile für sich entdeckt. Gerade die unsichtbare Gefahr im Internet zusammen mit den verheerenden Folgen eines Terrorangriffs weckt die Faszination vieler Menschen. Dies nutzen die Medien, indem sie den Begriff des Cyberterrorismus für jegliche Art von Cybercrime verwenden, um so die Aufmerksamkeit der Bevölkerung zu erlangen.[317] Durch diesen Umgang mit dem Terminus des Cyberterrorismus wird der Eindruck erweckt, dass cyberterroristische Taten jederzeit und überall Wirklichkeit werden.

Ein weiterer Grund für die unterschiedlichen Einschätzungen hinsichtlich der Gefahr vor Cyberterrorismus liegt in den unterschiedlichen Ansichten darüber, was genau sich hinter diesem Phänomen verbirgt. Wie bereits gezeigt, werden unter den Begriff des Cyberterrorismus sehr unterschiedliche terroristische Handlungen gefasst. Wird die

---

[314] So beispielsweise Stefen Cunnings, Leiter des „Centre for the Protection of National Infrastucture“ der britischen Regierung, auf einer Sicherheitskonferenz im April 2008, zitiert in: *Trevelyan*, Security experts split on „cyberterrorism“ threat, http://www.reuters.com/article/idUSL1692021220080416 (Stand: 25.05.2010).

[315] Zu diesem Ergebnis gelangt beipielsweise Michael Vatis, Leiter des „Institute for Security Technology Studies in der von ihm veröffentlichten Schrift „Cyber Attacs During the War on Terrorism: A Predictive Analysis; http://www.ists.dartmouth.edu/library/221.pdf (Stand: 25.05.2010).

[316] Beispielhaft hierzu: *ddp*, Geheimdienste befürchten Anschläge von Al Qaida auf das Internet, in: FAZ vom 30.März 2005; *Gellmann*: Cyber-Attacs by Al Qaeda Feard; terrorist at Threshold of Using Internet as Tools of Bloodshed, Experts say, in: washingtonpost vom 27.Juni 2002.

[317] *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 4

Nutzung des Internets als Logistikmittel ebenfalls als ein Fall des Cyberterrors gewertet, so muss auch die Gefahr für einen Angriff aus diesem Bereich höher eingeschätzt werden. Denn Terroristen nutzen bereits jetzt die Möglichkeiten, die ihnen das Internet zur Propaganda, Koordination, Planung oder Beschaffung finanzieller Mittel bietet.[318] Die Gefahr vor cyberterroristischen Angriffen ist allerdings dann anders zu bewerten, wenn, wie hier vertreten, nur der sogenannte „reine" Cyberterrorismus, also Angriffe mittels des Internets, unter das Wort Cyberterrorismus zu fassen ist. Ein solcher Anschlag ist nämlich bisher nicht bekannt geworden und es gibt auch keine haltbaren Hinweise darauf, dass Terrorgruppen das Internet als Waffe für sich entdeckt haben.[319] Andererseits zeigen Hackerangriffe auf das Internet immer wieder, wie verwundbar diese Infrastruktur ist. Im Moment mag die Gefahr vor einem cyberterroristischen Anschlag daher noch rein hypothetisch sein. Gerade aber in Hinblick auf die zunehmende weltweite Vernetzung und die Vorteile, die das Internet den Terroristen bietet, sollte das Phänomen Cyberterrorismus nicht aus den Augen verloren werden.

### *VI. Überblick über die Rechtsgrundlagen zur Bekämpfung des Cyberterrorismus in Europa*

Aufgrund der weltweiten Verfügbarkeit des Internets und der damit verbundenen grenzüberschreitenden Handlungsfähigkeit von Terroristen scheint es sinnvoll, in möglichst vielen verschiedenen Staaten einheitliche rechtliche Grundlagen zur Bekämpfung cyberterroristischer Tätigkeiten festzulegen. Auf Ebene der Europäischen Union finden sich keine Regelungen, die den Cyberterrorismus selbst, seine Definierung oder Bekämpfung, betreffen. Jedoch wurde das europäische Recht im Bereich des Terrorismus und im Bereich der Cyberkriminalität vereinheitlicht. So wurde im Jahre 2002 vom Europarat ein Rahmenbeschluss zur Terrorismusbekämpfung[320] erlassen, in dem unter anderem die Definition terroristischer Straftaten angeglichen wurde.[321] Computer- oder internetspezifische Aspekte finden sich in diesem Rahmenbeschluss jedoch nicht. Auch im Bereich der Cyberkriminalität wurden europäische Regelungen geschaffen. Die Wichtigsten davon finden sich in der Convention on Cybercrime[322] aus dem Jahre 2001 und dem Rahmenbeschluss des Europarats über Angriffe auf Informationssysteme[323] aus dem Jahr 2005. In beiden wurde die strafrechtliche Verfolgung von Cyberkriminalität bzw. von Angriffen auf Informationssysteme harmonisiert. Terroristische Aspekte sind

---

[318] vgl. hierzu: *Weimann*, Cyberterrorism. How real is the threat?, http://www.usip.org/files/resources/sr119.pdf (Stand: 25.05.2010), S. 3 ff.

[319] *Sieber/Brunst*, in: Council of Europe [Hrsg.], Cyberterrorism – the use of the Internet for terrorist purposes, 2007, S. 16.

[320] Rahmenbeschluss des Rates 2002/475/JI, ABl. EU Nr. L 164, S. 3.

[321] Siehe bereits unter I. 2.

[322] ETS Nr. 185.

[323] Rahmenbeschluss des Rates 2005/222/JI, ABl. EU Nr. L 69, S. 67.

nicht Inhalt dieser Regelungen. Es lässt sich demnach festhalten, dass auf europäischer Ebene Maßnahmen im Bereich der Cyberkriminalität und im Bereich des Terrorismus existieren. Bestimmungen, die beide Themen in Regelungen zum Cyberterrorismus zusammenführen, gibt es dagegen nicht. Da jedoch der Cyberterrorismus sowohl Elemente des Terrorismus als auch solche der Cyberkriminalität in sich vereint, können die Regelungen aus beiden Bereichen auf den Cyberterrorismus angewendet werden.[324] Trotz mangelnder spezieller Bestimmungen, gibt es demnach auf europäischer Ebene Regelungen, die bei Bekämpfung des Cyberterrorismus herangezogen werden können.

### *VII. Strafrechtliche Grundlagen zur Bekämpfung des Cyberterrorismus in Deutschland*

Die Bekämpfung von Cyberterrorismus kann sowohl im Vorfeld eines Anschlags als auch nach einem solchen, im Rahmen der strafrechtlichen Verfolgung der Täter, geschehen. Im folgenden Abschnitt wird die Frage geklärt werden, ob auch im deutschen Recht die Möglichkeit der strafrechtlichen Verfolgung von Cyberterrorismus besteht. In Deutschland finden sich, wie auch im europäischen Recht, keine Regelungen, die explizit den Cyberterrorismus betreffen. Vielmehr gibt es auch hier im Strafrecht Normen, deren Ziel die Bekämpfung von Computerkriminalität ist, und solche, die sich gegen Terrorismus richten. Zudem kommt für unterschiedliche Angriffsszenarien die Verwirklichung von weiteren spezifischen Straftatbeständen des StGB in Betracht. Fraglich ist jedoch, ob cyberterroristische, also mittels Computer und Internet durchgeführte, Angriffe überhaupt vom Tatbestand dieser Normen erfasst und damit mit dem deutschen Strafrecht bekämpft werden können. Im Folgenden werden nicht jegliche in Betracht kommende Regelungen des StGB auf ihre Anwendbarkeit hin überprüft. Vielmehr soll lediglich beispielhaft anhand einzelner Tatbestände ein Ansatzpunkt hinsichtlich dieser Fragestellung geboten werden.

#### *1. Verwirklichung von Tatbeständen zur Bekämpfung der Computerkriminalität*

##### *a) Ausspähen von Daten, § 202a StGB*

Ein cyberterroristischer Angriff könnte zunächst den § 202a StGB, das Ausspähen von Daten, verwirklichen. Dieser Tatbestand ist dann erfüllt, wenn sich die Täter unter Überwindung einer Zugangssicherung den Zugang zu Daten verschaffen, die nicht für sie bestimmt und gegen unberechtigten Zugang gesichert sind. Daten in diesem Sinne sind nach § 202a Abs. 2 StGB solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Ein Zugang verschafft sich derjenige, der durch seine Handlungen technische oder physische Einwirkungs-

[324] *Sieber/Brunst,* in: Council of Europe [Hrsg.], Cyberterrorism – the use of the Internet for terrorist purposes, 2007, S. 94, ausführlich S.50 ff.

möglichkeiten auf Datenspeicher oder einen physischen Zugang zum System erlangt.[325] Hiervon soll gerade das sogenannte Hacking, das Eindringen in fremde Computersysteme, mit umfasst werden.[326] Cyberterrorismus ist nach der hier vertretenen Ansicht ein rechtswidriger Angriff auf das Internet oder auf mit diesem verbundene Netzwerke und Infrastrukturen, der mittels Computer und Internet mit bestimmter Zielsetzung ausgeübt wird und den betroffenen Staat ernsthaft schädigt. Bei einem Angriff, bei dem Computersysteme kritischer Infrastrukturen manipuliert werden, wie es beispielsweise in den oben genannten Angriffsszenarien geschieht, erlangen die Terroristen technische Einwirkungsmöglichkeiten auf die Datenspeicher der betroffenen Systeme und verschaffen sich so Zugang i.S.d. § 202a StGB. Es kann im Fall einer cyberterroristisch motivierten Einwirkung auf Daten auch davon ausgegangen werden, dass die Daten nicht für die Täter bestimmt sind. Aufgrund ihrer wichtigen Bedeutung für den Staat werden Computersysteme kritischer Infrastrukturen in den meisten Fällen besonders gesichert sein, um einen unbefugten Zugriff zu verhindern. Damit liegen die Voraussetzungen des § 202a StGB vor. Ein cyberterroristischer Angriff wird also regelmäßig den Tatbestand dieser Vorschrift erfüllen.

*b) Datenveränderung, § 303a StGB*

Ein weiterer Tatbestand im StGB, der Angriffe gegen oder den Missbrauch von Computersystemen bekämpft, ist § 303a StGB. Ob ein cyberterroristischer Akt diesen Tatbestand erfüllt, richtet sich nach der konkreten Weise, in der die betroffenen Systeme manipuliert werden. § 303a StGB fordert die Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten. Der Verweis in § 303a StGB auf § 202a Abs. 2 StGB macht deutlich, dass nur solche Daten erfasst werden, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Die Daten müssen zudem für den Täter nach strittiger Ansicht fremd sein.[327] Ein Löschen von Daten ist dann gegeben, wenn die gespeicherten Daten vollständig und unwiederbringlich unkenntlich gemacht werden.[328] Unterdrückt werden Daten, sobald der Berechtigte dauerhaft oder für einen nicht unerheblichen Zeitraum nicht mehr auf sie zugreifen kann.[329] Die bestimmungsgemäße Gebrauchsfähigkeit wird durch das Unbrauchbarmachen aufgehoben[330], Verändern bedeutet eine Änderung des Informationsgehaltes oder des Aussagewertes der betroffenen Daten[331], beispielsweise eine inhaltli-

[325] Fischer, StGB, 56. Auflage (2009), § 202a Rn. 8.

[326] Fischer, StGB, 56. Auflage (2009), § 202a Rn. 1.

[327] Für diese Ansicht: Fischer, StGB, 56. Auflage (2009), § 303a Rn. 4; gegen diese Sichtweise: LK/*Wolff*, StGB, Band 10, 12. Auflage (2008), § 303a Rn. 8.

[328] Schönke/Schröder/*Stree*, StGB, 27. Auflage (2006), § 303a Rn. 4.

[329] LK/*Wolff*, StGB, Band 10, 12. Auflage (2008), § 303a Rn. 24.

[330] BT-Drs. 10/5058, S. 35; Fischer, StGB, 56. Auflage (2009), § 303a Rn. 11.

[331] Fischer, StGB, 56. Auflage (2009), § 303a Rn. 12.

che Umgestaltung[332]. Bei einem rechtswidrigen Angriff auf das Internet oder mit diesem verbundene Netzwerke und Infrastrukturen, wie er bei einem cyberterroristischen Angriff verübt wird, ist die Verwirklichung der Tathandlung denkbar. Werden wie in den oben genannten Szenarien Computersysteme manipuliert, so kann dies, beispielsweise im Fall der Einflussnahme auf Medikamenten- oder auf Lebensmittelzusammensetzungen, mittels inhaltlicher Umgestaltung und damit Veränderung fremder Daten geschehen. Die Verwirklichung des § 303a StGB durch cyberterroristische Angriffe ist demnach je nach Einzelfall möglich.

### *2. Verwirklichung von spezifischen Straftatbeständen bei unterschiedlichen Angriffsszenarien*

#### *a) Herbeiführung einer Explosion durch Kernenergie, § 307 StGB*

Cyberterroristen, die, wie im oben genannten Beispiel 4, in das Computersystem eines Kernkraftwerkes eindringen und dort computergesteuerte Abläufe oder Kontrollen in einer Weise manipulieren, dass eine Explosion durch Kernenergie verursacht wird, könnten den Tatbestand des § 307 StGB erfüllen. Dazu müssen sie durch das Freisetzen von Kernenergie eine Explosion herbeigeführt und Leib oder Leben eines anderen Menschen oder fremde Sachen von bedeutendem Wert gefährdet (Abs. 1) oder sogar qualifizierend den Tod eines Menschen verursacht haben (Abs. 3). Im genannten Szenario manipulieren die Täter das Computersystem eines Kernkraftwerkes, so dass durch das System eine große Menge Kernenergie freigesetzt und eine Explosion verursacht wird. Die kontrollierte Freisetzung von Kernenergie in Atomreaktoren fällt zwar nicht in den Anwendungsbereich des § 307 StGB[333]. Jedoch handelt es sich hier gerade nicht um eine kontrollierte Freisetzung, wie sie in Kernkraftwerken vorgesehen ist, sondern um eine bewusste Manipulierung gerade zur Herbeiführung einer Explosion. Das Herbeiführen solcher unkontrollierten Kernreaktionen fällt unter den Tatbestand der Vorschrift.[334] Dass bei einer solchen Tat durch Terroristen auch Menschenleben gefährdet, wahrscheinlicher sogar der Tod von Menschen herbeigeführt wird, kann ausgegangen werden. Damit erfüllt ein solcher cyberterroristischer Anschlag den Tatbestand des § 307 StGB.

#### *b) Herbeiführung einer Überschwemmung, § 313 StGB*

Auch ein Angriff auf das Computersystem einer Staumauer, wodurch die computergesteuerten Tore geöffnet werden, wie oben unter Beispiel 5, könnte eine Bestrafung nach dem StGB nach sich ziehen. In Betracht kommt hier vor allem § 313 StGB, der die

[332] LK/*Wolff*, StGB, Band 10, 12. Auflage (2008), § 303a Rn. 27.
[333] Schönke/Schröder/*Stree*, StGB, 27. Auflage (2006), § 307 Rn. 3.
[334] LK/*Wolff*, StGB, Band 11, 12. Auflage (2008), § 307 Rn. 2.

Herbeiführung einer Überschwemmung unter Strafe stellt. Die Voraussetzungen hierzu sind, dass die Terroristen eine Überschwemmung herbeiführen und das Leben eines Menschen oder fremde Sachen von bedeutendem Wert konkret gefährden. Wird eine größere Fläche oder ein Raum bestimmungswidrig überflutet, weil eine große Menge Wasser über seine natürlichen oder künstlichen Grenzen austritt, und dadurch zu einer Gefahr für alle im betroffenen Gebiet befindlichen Personen oder Sachen wird, so stellt dies eine Überschwemmung dar.[335] Werden die Tore einer Staumauer durch Terroristen geöffnet, so fließt das gestaute Wasser in großer Menge und mit viel Kraft aus dem Staubecken heraus und verursacht zwangsläufig eine Überschwemmung. Mit welchen Mitteln die Überschwemmung herbeigeführt, also verursacht, wird, ist im Rahmen des § 313 StGB gleichgültig.[336] Daher kann auch eine Manipulation des Computersystems der Staumauer, wodurch die Öffnung der Tore bewirkt wird, als Herbeiführen i.S.d. § 313 StGB gewertet werden. Ebenso kann bei einer solchen Tat durch Terroristen davon ausgegangen werden, dass Menschenleben konkret gefährdet werden. Daher kann § 313 StGB in einem solchen Fall auch auf eine cyberterroristische Tat verwirklicht werden.

### *c) Angriff auf Luft- und Seeverkehr, § 316c StGB*

Auch das oben dargestellte Beispiel 3, in dem Cyberterroristen in das Computersystem der Flugsicherheitsüberwachung eindringen, mittels Computer die Kontrolle über zwei Passagierflugzeuge übernehmen und diese kollidieren lassen, könnte einen spezifischen Tatbestand aus dem StGB verwirklichen. Hier kommt eine Bestrafung nach § 316c Abs. 1 Nr. 1a), Nr. 2 StGB in Betracht, wenn die Terroristen Gewalt anwenden oder sonstige Machenschaften vornehmen, um die Herrschaft über ein im zivilen Luftverkehr eingesetztes und im Flug befindliches Luftfahrzeug zu erlangen oder auf dessen Führung einzuwirken, oder um ein solches Luftfahrzeug zu zerstören. Die angewandte Gewalt kann sich gegen Menschen, aber auch gegen Sachen richten.[337] Unter Machenschaften ist vor allem die Beeinflussung der an Bord des Flugzeugs befindlichen Geräte mit technischen Mitteln zu verstehen.[338] In dem hier in Frage stehenden Fall dringen die Täter in ein Computersystem ein und übernehmen so mittels Computer die Kontrolle über zwei Passagierflugzeuge. Diese werden zerstört, in dem eine Kollision herbeigeführt wird. Damit erlangen die Cyberterroristen die Herrschaft über die Flugzeuge, wirken auf ihre Führung ein und zerstören sie. Dies geschieht zwar nicht unter Anwendung von Gewalt, jedoch manipulieren die Täter mittels eines Computers die Steuerungsgeräte des Flugzeugs und begehen damit Machenschaften i.S.d. § 316c StGB. Cyberterroris-

[335] Fischer, StGB, 56. Auflage (2009), § 313 Rn. 2.
[336] Schönke/Schröder/*Stree*, StGB, 27. Auflage (2006), § 313 Rn. 4.
[337] LK/*Wolff*, StGB, Band 11, 12. Auflage (2008), § 316c Rn. 20 ff.
[338] Fischer, StGB, 56. Auflage (2009), § 316c Rn. 6.

ten können bei Umsetzung dieses Szenarios demnach nach § 316c StGB strafrechtlich verfolgt werden.

*3. Verwirklichung des Tatbestandes zur Bekämpfung des Terrorismus, § 129a StGB*

Im StGB findet sich mit § 129a auch eine Norm, die der Bekämpfung des Terrorismus dient. Da jedoch auch in dieser Vorschrift der Cyberterrorismus als solcher nicht genannt ist, stellt sich ebenfalls die Frage, ob eine Anwendung möglich ist. § 129a StGB bestraft in Abs. 1 zum einen die Gründung von Vereinigungen, deren Zweck darauf gerichtet ist, besonders schwerwiegende Straftaten zu begehen, zum anderen die Mitgliedschaft in einer solchen Vereinigung. In einer abschließenden Aufzählung werden die in Frage kommenden Straftaten aufgeführt. Dazu gehören unter anderem Mord (§ 211 StGB), Totschlag (§ 212 StGB), Erpresserischer Menschenraub (§ 239a StGB) und Geiselnahme (§ 239b StGB). Auch in Abs. 2 wird die Gründung von Vereinigungen, deren Zweck darauf gerichtet ist, eine in diesem Absatz genannte Katalogtat zu begehen, unter Strafe gestellt. Genannt sind hier unter anderem §§ 226, 303b, 307, 313, 316c StGB. In Absatz zwei wird die Strafbarkeit darüber hinaus noch an weitere Bedingungen geknüpft. Die Taten müssen dazu bestimmt sein, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung von Gewalt zu nötigen oder die politischen verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen. Zudem müssen die Taten nach dem Wortlaut der Vorschrift erhebliche Schäden anrichten. Vor allem durch die zuletzt genannten Voraussetzungen zeigt sich, dass insbesondere Abs. 2 durch den bereits angesprochenen europäischen Rahmenbeschluss zur Terrorismusbekämpfung[339] beeinflusst ist. Nach § 129a Abs. 3 StGB werden schließlich auch jene Vereinigungen erfasst, deren Zweck darauf gerichtet ist, mit den in den Abs. 1 und 2 genannten Straftaten zu drohen. Unabhängig von den im Einzelnen umstrittenen Begriffsbestimmungen der Norm, beispielsweise die der Vereinigung[340], lässt sich feststellen, dass eine Anwendbarkeit der Vorschrift des § 129a StGB je nach konkreter Tat auch auf cyberterroristische Anschläge möglich ist. Terrorismus ist ein Grundelement des Cyberterrors. Daher sind die wesentlichen Merkmale, nämlich die Begehung einer rechtswidrigen Tat, die ernsthafte Schädigung sowie die politisch motivierte Zielsetzung, bei beiden Phänomenen identisch. Diese Merkmale werden auch in § 129a StGB vorausgesetzt. Werden also durch den Cyberterrorismus Katalogtaten nach § 129a Abs. 1 oder Abs. 2 StGB verwirklicht, so sind die Voraussetzungen des § 129a StGB erfüllt. Zu denken sind hier vor allem an Taten nach §§ 307, 313, 316c StGB.[341]

[339] Vgl. oben II. 1.
[340] Siehe hierzu zum Beispiel Fischer, StGB, 56. Auflage (2009), § 129a Rn. 4f.
[341] Vgl. VII. 2.

Dass diese mittels Computer und Internet und nicht beispielsweise mittels Sprengstoff durchgeführt werden, ist gleichgültig, da im Rahmen des § 129a StGB das Mittel, mit dem die Katalogtaten verwirklicht werden, keine Rolle spielt. § 129a StGB kann somit auch im Falle von Cyberterrorismus zur Anwendung kommen.

### *4. Ergebnis*

Es hat sich gezeigt, dass ein cyberterroristischer Angriff, auch wenn er im deutschen Strafrecht nicht ausdrücklich unter Strafe gestellt ist, verschiedene Tatbestände des StGB erfüllen kann. Sowohl Normen, die sich gegen Computerkriminalität richten und keinerlei terroristische Komponenten aufweisen, als auch die Vorschrift zur Bekämpfung des Terrorismus erfassen Fälle des Cyberterrorismus. Zudem können unterschiedliche Angriffe auch spezifische Straftatbestände erfüllen. Damit bietet das StGB verschiedene Möglichkeiten der strafrechtlichen Bekämpfung von Cyberterrorismus.

## *VIII. Fazit*

Der Cyberterrorismus ist ein Phänomen, das immer wieder in der öffentlichen Diskussion auftaucht. Vor allem in Zeiten der weltweiten Vernetzung durch das Internet gewinnt die Frage nach seiner Bekämpfung immer größere Bedeutung. In Hinblick auf eine Begriffsbestimmung erscheint es sinnvoll, dass auch der Cyberterrorismus die Merkmale des traditionellen Terrorismus, nämlich einen rechtswidrigen Angriff mit erheblicher Schädigung und politisch motivierter Zielsetzung einschließt. Zudem sollten nur Angriffe auf bzw. mittels des Internets von der Definition umfasst werden, um eine Unterscheidbarkeit zum traditionellen Terrorismus zu erreichen. Im Gegensatz zu diesem ist bisher noch kein Fall von Cyberterror bekannt geworden. Aufgrund der vielen Vorteile, die das Internet den Terroristen bietet und der immer weiter reichenden Vernetzung sollte die Gefahr vor Anschlägen durch Cyberterroristen nicht aus den Augen verloren werden. Es gibt jedoch bereits jetzt auf nationaler sowie auf internationaler Ebene Normen zur Bekämpfung von Computerkriminalität oder von Terrorismus, die auch den Cyberterror erfassen. Damit kann rechtlich gegen dieses Phänomen vorgegangen werden.

## Kapitel 5: Automated Content Generation

*C. Jones*

*Automated Content Generation* (oder auch *Computer Generated Content*[342]) als Phänomen im modernen Internet bedeutet, dass Texte ohne oder mit nur minimalem Einwirken des Benutzers erstellt und auf Webseiten veröffentlicht werden. Ziel ist es üblicherweise, auf den jeweiligen Webseiten Werbeanzeigen zu schalten und daraus Einnahmen zu erzielen.

### *I. Merkmale des Automated Content Generation*

Kern des Automated Content Generation ist das Generatorprogramm, das mittels eines Algorithmus nach Vorgabe des Benutzers Texte beliebiger Länge erstellt. Hierbei sind drei methodische Richtungen zu unterscheiden:

Einmal können Texte mittels eines Zufallsgenerators basierend auf entsprechenden Wörterbüchern, Satzbausteinen und Grammatikregeln generiert werden. Dabei werden aus einer bestehenden Datenbank nach geeigneten Auswahl- und Zusammensetzungsregeln verschiedene Textbausteine und Wörter so zusammengefügt, dass ein lesbarer, in sich abgeschlossener und grammatikalisch korrekter Text entsteht. Je nach Ausgereiftheit des Programmes und Eingrenzung des Themas variiert der inhaltliche Anspruch dabei von völliger Inhaltsleere bis zu durchaus informativen oder zumindest unterhaltsamen Kurztexten, natürlich begrenzt durch den Umfang der zugrunde liegenden Datenbanken.[343]

Auch ist es möglich, aus vorhandenen Texten einen neuen bzw. neu erscheinenden Text zu erstellen. Dazu können einzelne Sätze oder Abschnitte aus verschiedenen Quellen ohne weitere Umgestaltung zu einem neuen Text zusammengefügt werden („Scraping"), einzelne Wörter und Phrasen eines Textes können durch Synonyme ausgetauscht werden („Thesaurus substitution") oder es werden aus den vorhandenen Abschnitten durch statistische Modelle neue Texte zusammengefügt (z.B. „Markov chains").[344] Auch Kombinationen dieser Techniken sind möglich.

---

[342] Content (Inhalt) bezieht sich dabei auf veröffentlichte Webseiten. Automated Content Generation kann als Unterfall der Textgenerierung bzw. natürlichsprachlichen Generierung (Natural Language Generation, NLG) betrachtet werden.

[343] Unter http://pdos.csail.mit.edu/scigen/ lassen sich beispielsweise englische Fachtexte aus dem Bereich der Informatik generieren, die für Experten leicht als Fälschung zu erkennen sind, auf den ersten Blick aber echt erscheinen.

[344] Vgl. http://www.aiplayground.org/artikel/markov/; http://www.slightlyshadyseo.com/index.php/the-basics-of-content-generation-methods-coherrence-and-unique-content/ (01.05.2010).

Die dritte, weit fortgeschrittenere Vorgehensweise, setzt „intelligente“ Programme ein, die qualitativ weitaus hochwertigere Texte erstellen können.[345] Diese Programme sind unter anderem in der Lage, über das Internet aus Nachrichtenseiten oder Wissensdatenbanken selbsttätig Fachvokabular und relevante Informationen über ein gewünschtes Thema zu extrahieren. Durch programmierte Grammatikregeln und künstliche Intelligenz können daraus neue Texte generiert werden. Da beliebig viele Quellen herangezogen werden können, kann – entsprechend fortgeschrittene Software vorausgesetzt – ein Produkt erzeugt werden, das nicht von menschlich erstellten Texten zu unterscheiden ist.

Die so erstellten Texte werden manuell oder wiederum automatisch auf Webseiten, Foren oder Blogs veröffentlicht, auf denen auch Werbung eingeblendet wird. Die Einnahmen sind dabei abhängig von der Anzahl der Besucher der Webseiten bzw. der Anzahl an Aufrufen der Werbeanzeigen („Werbeklicks“).[346] Entscheidend ist daher auch die Platzierung der Webseite bei relevanten Suchmaschinen. Je fachspezifischer und umfassender die Informationen auf den Webseiten sind und je häufiger etwa Blogs mit neuen Beiträgen aktualisiert werden, desto höher wird die Seite bei Suchmaschinen gelistet und bei Eingabe entsprechender Suchbegriffe angezeigt. Daher werden zusätzlich auch Technologien zur Suchmaschinenoptimierung[347] eingesetzt, was zu erhöhten Besucherzahlen der Webseiten und damit höheren Werbeeinnahmen führt.

### *II. Urheberrechtliche Bewertung*

Bei einer urheberrechtlichen Betrachtung sind zwei Aspekte zu unterscheiden. Zunächst ist fraglich, ob ein durch Automated Content Generation erstellter Text selbst urheberrechtlich geschützt ist. Des Weiteren ist zu untersuchen, ob die automatische Erstellung eines solchen Textes unter Verwendung fremder Texte deren Urheberrechte verletzen kann.

#### *1. Eigener urheberrechtlicher Schutz*

Nach § 1 UrhG sind nur Werke der Literatur, Wissenschaft und Kunst durch das Gesetz über Urheberrecht und verwandte Schutzrechte geschützt, worunter nach § 2 Abs. 1 Nr. 1 UrhG auch Sprachwerke wie Schriftwerke zählen. Da Computerprogramme nach

---

[345] So etwa Programme auf http://www.kwikcontent.com; http://www.smartarticlegenerator.com; http://www.contentfx.com (25.05.2010), wobei zukünftig mit noch weiter entwickelten Technologien zu rechnen ist.

[346] Vgl. zum Hauptanwendungsfall der kontextbezogenen Suchmaschinenwerbung Kilian/Heussen/*Egermann*, Computerrechts-Handbuch, 27. Aufl. 2009, Absch. 3, Suchmaschinen, Rn. 18.

[347] Vgl. dazu *Geßner*, Marken- und lauterkeitsrechtliche Probleme der suchmaschinenbeeinflussenden Verwendung von Kennzeichen, 2008; Hoeren/Sieber/*Hoeren*, Handbuch Multimedia-Recht, 2008 Zur technischen Seite *Promny*, Grundlagen der Suchmaschinenoptimierung, 2009

dem Willen des Gesetzgebers den Sprachwerken zuzuordnen sind (§ 69a Abs. 4 UrhG),[348] unterfällt zumindest das Generatorprogramm selbst ohne weiteres dem urheberrechtlichen Schutz.

Weniger eindeutig lässt sich die generierte Webseite einordnen. Grundsätzlich sind Werke nach dem UrhG nur geschützt, wenn es sich um persönliche geistige Schöpfungen handelt, § 2 Abs. 2 UrhG. Sofern eine Webseite ausschließlich auf Suchmaschinen ausgerichtet und nicht zur menschlichen Wahrnehmung bestimmt ist (also etwa weißer Text auf weißem Hintergrund), erscheint es vertretbar, im Einzelfall unabhängig von der Art ihrer Erstellung die Voraussetzungen der Schöpfungshöhe und damit die Werkqualität von vornherein abzulehnen.[349]

Auch sind reine Zufallserzeugnisse und maschinell generierte Produkte ohne Zutun menschlichen Schaffens grundsätzlich nicht urheberrechtlich geschützt.[350] Jedoch kann auch dann eine geistige Schöpfung vorliegen, wenn Hilfsmittel zur Erstellung des Produktes verwendet werden.[351] Dies ist insbesondere der Fall, wenn der Urheber das Werk durch das von ihm geschaffene Computerprogramm persönlich gestaltet oder geplante und zufällige Elemente kombiniert.[352] Die reine Initiative zur Schaffung eines Werkes reicht dabei nicht aus, die Auswahl der Form und des Inhalts selbst darf nicht überwiegend vom Programm durchgeführt werden.[353] Hier kommt es im Einzelfall darauf an, wie weit der Benutzer von Textgeneratoren noch menschlich-gestalterische Aktivität entfaltet.[354] Zu denken ist etwa an eine manuelle Auswahl und Nachbearbeitung der generierten Texte, die Illustration mit Bildern oder die Zusammenstellung zu einem Sammel- oder Datenbankwerk[355] (§ 4 UrhG).

### *2. Verletzung des Urheberrechts der Quelltexte*

Je nach Ausgestaltung kann das intelligente Generatorprogramm in der Lage sein, sich selbsttätig mit relevanten Informationen über das Thema zu versorgen. Es ist technisch möglich, dass das Programm automatisch verschiedene Suchmaschinen abfragt,

---

[348] Vgl. Wandtke/Bullinger/*Grützmacher*, Praxiskommentar zum Urheberrecht, 3. Aufl. 2009, § 69a Rn. 2; HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 15 Rn. 10.

[349] *Bernreuter*, WRP 2008, 1057, 1063 f.

[350] HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 2 Rn. 24; Schricker/*Loewenheim*, Urheberrecht, 3. Aufl. 2006, § 2 Rn. 12.

[351] Wandtke/Bullinger/*Bullinger*, Praxiskommentar zum Urheberrecht, 3. Aufl. 2009, § 2 Rn. 15 f.

[352] Wandtke/Bullinger/*Bullinger*, Praxiskommentar zum Urheberrecht, 3. Aufl. 2009, § 2 Rn. 16 f.; kritischer Schricker/*Loewenheim*, Urheberrecht, 3. Aufl. 2006, § 2 Rn. 11.

[353] HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 2 Rn. 26; Schricker/*Loewenheim*, Urheberrecht, 3. Aufl. 2006, § 2 Rn. 14, m.w.N.

[354] Schon dem Ansatz gegenüber kritisch HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 2 Rn. 28.

[355] Zu den einzelnen Voraussetzungen HK-UrhR/*Kotthoff*, 2. Aufl. 2008, § 4 Rn. 6 ff.

einzelne Ergebnisseiten besucht und dort relevante Textabschnitte und Einzelinformationen herausfiltert.

Der Ersteller der Quellseiten hat als Urheber das ausschließliche Verwertungs- und Vervielfältigungsrecht (§§ 15, 16 ff UrhG). Eine Schranke findet dieses Recht unter anderem im Zitatrecht (§ 51 UrhG).[356] Das Regelbeispiel des sog. Kleinzitats (§ 51 S. 2 Nr. 2 UrhG) setzt dabei die Aufnahme in ein selbständiges Sprachwerk voraus, ist also nur anwendbar, wenn der generierten Seite selbst Werkqualität zukommt.[357] Das Zitat muss dann als solches kenntlich gemacht werden, der zitierte Text darf gerade nicht, wie beim Automated Content Generation üblich, als eigenes Werk ausgegeben werden.[358] Vielmehr muss eine innere Verbindung mit eigenen Gedanken hergestellt werden. Das Zitat soll nicht selbst Inhalt sein, sondern selbständige Ausführungen des Zitierenden unterstützen.[359] Zudem ist das Gebot der Quellenangabe nach § 63 Abs. 1 und 2 UrhG zu beachten. Ein Verwender von Automated Content Generation wird sich daher regelmäßig nicht auf das Zitierrecht nach § 51 UrhG stützen können.

Das Urheberrecht schützt allerdings nur die konkrete Erscheinungsform eines Werkes.[360] Wird also nicht unmittelbar aus den fremden Textbausteinen, sondern nur aus den darin enthaltenen Informationen ein völlig eigener Text generiert, wird dann das ursprüngliche Werk nicht vervielfältigt.[361] Dies ist auch der Fall, wenn intelligente Generatorenprogramme neue Inhalte erstellen, ohne Textteile aus bereits bestehenden Webseiten oder veröffentlichten Texten zu übernehmen, etwa indem sie aus einzelnen Passagen lediglich die Satzkonstruktionen und das Fachvokabular sammeln, extrahiert und nach den im Programm festgelegten Satzkonstruktionsregeln neu zusammenstellen.

Es kann sich dabei jedoch um eine Umgestaltung (§ 23 UrhG) handeln, die nicht ohne Einwilligung des ursprünglichen Urhebers veröffentlicht werden darf. Unter Umgestaltungen werden Handlungen verstanden, bei denen das Werk in abgeänderter Form genutzt wird,[362] sofern von einem Programm mehr als die bloßen Ideen übernommen

---

[356] Zur Anwendbarkeit im Internet *Bisges*, GRUR 2009, 730.

[357] HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 51 Rn. 9, 35, der die Werkqualität des zitierenden Werkes als generelle Voraussetzung des § 51 UrhG sieht.

[358] *OLG München*, NJW 1999, 1975; HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 51 Rn. 15.

[359] BGHZ 28, 234, 239 f; BGH, GRUR 1987, 34, 35; HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 51 Rn. 14.

[360] Wandtke/Bullinger/*Bullinger*, Praxiskommentar zum Urheberrecht, 3. Aufl. 2009, § 2 Rn. 33; zur Anwendbarkeit der §§ 16 ff auf Internet und neue Medien HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 15 Rn. 27 f.

[361] Anders jedoch bei (etwa nur in Verwendungskontext, Größe, Zuschnitt oder Qualität veränderten) Bildern, vgl. *Ernst*, MR-Int 2009, 1 ff.

[362] *BGH*, GRUR 1990, 669, 673; *BGH*, GRUR 2002, 532, 534.

werden[363] und es sich nicht um eine zulässige und genehmigungsfreie Benutzung (§ 24 UrhG) handelt.

Eine freie Benutzung (§ 24 UrhG) kann wiederum nur vorliegen, wenn der generierte Text ein Werk im Sinne des § 2 UrhG ist.[364] Weitere Voraussetzung ist, dass der generierte Text gegenüber der Vorlage völlig neue Wege geht und im Vergleich als selbständiges Werk gilt,[365] was im Rahmen einer Gesamtschau festgestellt wird[366]. Da viele Automated Content Generator-Programme unzählige Vorlagentexte in kaum nachvollziehbarer Weise vermischen, kann dies im Einzelfall zu bejahen sein. Wird diese Schwelle nicht erreicht, und lassen sich Elemente des Ausgangswerks im generierten Text nachweisen,[367] handelt es sich um eine Umgestaltung.

### *III. Fazit*

Automatisch generierte Texte können im Einzelfall urheberrechtlichen Schutz genießen, wenn eine gewisse schöpferische Leistung des Erstellers vorhanden ist. Werden Quelltexte zur Erstellung herangezogen, lässt sich dann auch eine freie – und damit zulässige – Benutzung der Originaltexte annehmen. Erreicht der generierte Text jedoch nicht selbst Werkqualität, so genießt der Urheber der Quelldokumente Schutz vor der Ausbeutung seiner Leistung auch durch automatische Umgestaltung. Inwieweit darüber hinaus durch die Nutzung automatisch generierter Texte die Vertragsbestimmungen der Werbepartner verletzt werden, ist von den jeweiligen vertraglichen Vereinbarungen abhängig.

[363] HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 23 Rn. 5.
[364] Vgl. HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 24 Rn. 7; Schricker/*Loewenheim*, Urheberrecht, 3. Aufl. 2006, § 24 Rn. 9.
[365] *BGH*, GRUR 1963, 40, 42; Schricker/*Loewenheim*, Urheberrecht, 3. Aufl. 2006, § 24 Rn. 10 f.
[366] *BGH*, NJW 2000, 2202, 2206; Schricker/*Loewenheim*, Urheberrecht, 3. Aufl. 2006, § 24 Rn. 12.
[367] Vgl. *BGH*, NJW 1970, 250, 251; HK-UrhR/*Dreyer*, 2. Aufl. 2008, § 3 Rn. 13.

# Kapitel 6: Ubiquitäres Computing

*S. Röchner*

## *I. Begriff des Ubiquitären Computing*

Der Begriff des Ubiquitären Computing wurde Anfang der 1990er Jahre von Mark Weiser geprägt, der damit eine Vision beschrieb, in der der heute noch verbreitete Personalcomputer verschwindet und stattdessen allgegenwärtige, unsichtbare Computer die Menschen bei ihren Tätigkeiten unterstützen.[368] Heutzutage versteht man unter Ubiquitärem Computing die Allgegenwärtigkeit von Computerleistung und Informationstechnik.[369] Viele Alltagsgegenstände werden mit Sensoren sowie mit Informations- und Kommunikationstechnik ausgestattet. Auf diese Weise können die Gegenstände mittels der Sensoren Informationen aus ihrer Umgebung aufnehmen, diese speichern und automatisch verarbeiten. Außerdem ist es den verschiedenen Objekten dank der Kommunikationstechnik möglich, Daten auszutauschen und miteinander zu kommunizieren. Aufgrund dieses Zusammenspiels kann eine Reaktion auf die wahrgenommene Umgebung ausgelöst werden. Computer sollen so auf unauffällige Weise den Menschen im Alltag unterstützen.[370]

Kennzeichnend für das Ubiquitäre Computing sind die Merkmale der Einbettung, der Energieautarkie, der Vernetzung, der Kontextsensitivität, der Autonomie und der Allgegenwärtigkeit.[371] Die Hardware-Komponenten, die die Informations- sowie die Kommunikationstechnik tragen, sind so klein, dass sie in viele Alltagsgegenstände eingebettet werden können. Um eine dauerhafte Nutzung der Technik zu ermöglichen, ist es notwendig, den Energieverbrauch zu optimieren und eine unabhängige, mobile Energieversorgung ermöglichen. Die verschiedenen Gegenstände sind miteinander vernetzt und können bei Bedarf untereinander kommunizieren. Durch diese Kommunikation mit anderen und mit Hilfe ihrer Sensoren können die Objekte Informationen über ihre Umgebung aufnehmen und diese verarbeiten. Diese Fähigkeit wird als sogenannte Kontextsensitivität bezeichnet.[372] Auf die gefundenen Informationen können die in den Alltagsgegenständen integrierten Computer dann autonom, also selbstständig und automatisch, reagieren. Im Ubiquitären Computing ist dieses Zusammenspiel aus Sensoren und In-

---

[368] *Mattern*, Ubiquitous Computing – Die Vision von der Informatisierung der Welt, http://www.vs.inf.ethz.ch/publ/papers/UbicompLogin.pdf (Stand: 28.05.2010).

[369] *Bundesministerium für Bildung und Forschung [Hrsg.]*, TAUCIS. Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung, 2006, S. 11.

[370] Zu möglichen Anwendungsfeldern siehe III.

[371] Ausführlich hierzu DT-Drs. 17/405, S. 22.

[372] *Bundesamt für Sicherheit in der Informationstechnik [Hrsg.]*, Risiken und Chancen des Einsatzes von RFID-Systemen, 2005, S. 17.

formation- und Kommunikationstechnik allgegenwärtig. Von einer Vielzahl von Anbietern und Betreibern werden verschiedene Systeme mit unterschiedlichen Dienstleistungen bereitgestellt. So kann die Technik jeder Zeit und an jedem Ort in unauffälliger Weise ihren Nutzer unterstützen. Noch ist diese allgegenwärtige Vernetzung des Ubiquitären Computing keine Realität.[373] Vielmehr gibt es erst einzelne voneinander unabhängige Systeme, in denen eine Informations- und Kommunikationstechnik eingesetzt wird. Ein umfassender Einsatz dieser Technologien, der alle Lebensbereiche des Menschen erreicht, bleibt vorerst eine Vision.

### *II. Überblick über die technische Grundlagen*

Im Ubiquitären Computing werden verschiedene Techniken vereint. So ist der Einsatz von Mikroprozessoren erforderlich, aber auch der von drahtlosen Funktechniken sowie Datenübertragungen durch universale Netze.[374] In einem System des Ubiquitären Computing lassen sich daher aus technischer Sicht mehrere grundsätzliche Elemente unterscheiden, die zum Funktionieren des Systems notwendig sind.[375] Um Informationen aufnehmen zu können, müssen zunächst an Alltagsgegenständen aber auch in der Umwelt Sensoren oder Eingabemöglichkeiten existieren, mit Hilfe derer die Umwelt automatisch oder mittels Eingabe erfasst werden kann. Alle gefundenen Informationen werden dann auf dem Endgerät des Nutzers lokal oder auf dem Server des Anbieters zentral gesammelt, verarbeitet und gespeichert. Die hierfür erforderliche Datenübertragung erfolgt über eine ebenfalls verteilte, zumeist drahtlose, Kommunikationsinfrastruktur. In Hintergrundsystemen oder auch im Endgerät kommen schließlich so genannte „intelligente Verfahren“[376] zum Einsatz. Diese werten die aktuell übermittelten Daten des jeweiligen Gegenstandes, bereits gespeicherte Daten aber auch Daten aus externen, also nicht dem Ubiquitären-Computing-System angehörigen Datenbeständen, wie beispielsweise dem Internet, aus. Anhand all dieser Informationen entscheiden sie dann, ob eine Aktion ausgelöst werden sollte oder nicht.

Verwirklichen lässt sich diese Allgegenwärtigkeit von Computern mit verschiedenen Methoden. Zwar findet bisher ein umfassender Einsatz von Computertechnik im Alltagsleben noch nicht statt, jedoch gibt es bereits jetzt unterschiedliche Systeme, die bestimmte Merkmale des Ubiquitären Computings verwirklichen. Als prototypisch für Ubiquitäre-Computing-Systeme können beispielsweise Sensor- und Ad-hoc-Netze, Location-based Services oder RFID-Systeme (Radio-Frequenz-Identifikations-Systeme)

---

[373] Vgl. BT-Drs. 17/405, S. 19.

[374] *Bundesamt für Sicherheit in der Informationstechnik [Hrsg.]*, Risiken und Chancen des Einsatzes von RFID-Systemen, 2005, S. 10.

[375] Zum Folgenden siehe: BT-Drs. 17/405, S. 28.

[376] BT-Drs. 17/405, S. 28.

betrachtet werden.[377] In Sensornetzen überwachen Sensoren selbstständig ihre Umgebung und übermitteln die gewonnenen Daten an die Nutzer des Systems.[378] Ad-hoc-Netze sind Funknetze, die mehrere Geräte ohne feste Infrastruktur oder vermittelnde Dienste zu einem Netzwerk verbinden.[379] Unter Location-based Services versteht man die Bereitstellung von Diensten unter Einbeziehung der Positionsdaten des Nutzers.[380] Ein RFID-System schließlich ist ein Verfahren zur automatischen Identifizierung einer Person oder einer Sache über Funk.[381] All diese Technologien können bis jetzt noch nicht zu einem allgegenwärtigen Netz von unterstützenden Computern ausgebaut werden. Doch eine Weiterentwicklung und das Zusammenwirken der verschiedenen Systeme kann in der Zukunft zur Verwirklichung des Ubiquitären Computing führen.

Das RFID-System gilt dabei als Schlüsseltechnologie des Ubiquitären Computing[382] und soll deshalb kurz in seiner Funktionsweise dargestellt werden. Die wichtigsten Komponenten des RFID-Systems sind der Transponder, auch Tag genannt, und ein Lesegerät.[383] Der Transponder besteht aus einem elektronischem Mikrochip und einer Antenne, das Lesegerät aus Sender, Empfänger, Antenne und eventuell einer Schnittstelle.[384] Das Tag mit auf dem Chip gespeicherten Informationen, beispielsweise eine individuelle Seriennummer, wird zunächst in einen Gegenstand integriert. Das Lesegerät sendet Funksignale, die vom Transponder empfangen werden können. Sobald dieser mittels seiner Antenne erkennt, dass er sich im Bereich des Lesegerätes befindet, schickt er die auf seinem Chip enthaltenen Informationen an das Gerät, das sie erfasst und speichert. Über die Schnittstellen können die Lesegeräte die Daten auch an andere Systeme weiterleiten, damit dort eine Verarbeitung der Daten stattfinden kann. Auf diese Weise ist es möglich, die mit Transpondern ausgestatteten Gegenstände automatisch zu identifizieren. Da die Identifizierung von Sachen oder Menschen genauso wie die Einsetzung von Sensoren zur automatischen Erfassung der Umgebung und der Austausch von Informationen in einem Netzwerk Teil des Ubiquitären Computing sind, können die im voran stehenden Absatz genannten Systeme, einen Eindruck darüber vermitteln, wie die Vision des Ubiquitären Computing technisch umsetzbar ist.

---

[377] *Bundesministerium für Bildung und Forschung [Hrsg.]*, TAUCIS. Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung, 2006, S. 14.

[378] BT-Drs. 17/405, S. 7.

[379] BT-Drs. 17/405, S. 30.

[380] *Bundesministerium für Bildung und Forschung [Hrsg.]*, TAUCIS. Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung, 2006, S. 14.

[381] *Bundesamt für Sicherheit in der Informationstechnik [Hrsg.]*, Risiken und Chancen des Einsatzes von RFID-Systemen, 2005, S. 17.

[382] *Conrad*, CR 2005, 537 (544).

[383] *Conrad*, CR 2005, 537.

[384] *Holznagel/Bonnekoh*, MMR 2006, 17.

### *III. Mögliche Anwendungsfelder*

Die denkbaren Anwendungsgebiete des Ubiquitären Computing sind vielfältig. Einen Hinweis darauf, wie ein solches System funktionieren kann, findet sich bei einer Betrachtung von RFID-Systemen, die bereits heute getestet werden. Der Einsatz der RFID-Technologie bietet sich beispielsweise im Handel an.[385] Dort können die Produkte mit Mikrochips ausgestattet werden. Auf ihnen werden Informationen zu Preis, Inhaltsstoffen oder auch Empfehlungen für andere jeweils passende Produkte gespeichert. Lesegeräte finden sich in den Lagern und Regalen, an der Kasse und an den Einkaufswägen. Sobald eine Ware aus dem Lager in ein Regal gebracht wird, erkennen dies die Geräte im Lager und im Regal und speichern diese Information. Fehlt ein Produkt an einer Stelle, so wird dieser Umstand automatisch gemeldet oder sogar selbstständig eine Nachbestellung über ein verbundenes Netzwerk durchgeführt. Auch wenn ein Kunde eine Ware aus dem Regal nimmt und in seinen Einkaufswagen legt, wird dies durch die Lesegeräte wahrgenommen. Über die Geräte im Wagen können Kunden die Informationen über den Preis oder zu den Inhaltsstoffen auslesen. Im Kassenbereich erkennt ein weiteres Lesegerät automatisch die Waren, die sich im Wagen befinden, und erstellt dementsprechend eine Rechnung. Auf diese Weise werden die Abläufe im Handel effizienter gestaltet.

Ein weiteres Beispiel für die Anwendung der RFID-Technologie findet sich im sogenannten Ticketing. Hier werden Personen beispielsweise für den Besuch eines Großereignisses automatisch identifiziert.[386] Angewandt wurde ein solches Verfahren bei der Vergabe der Tickets zur FIFA Fußball WM 2006.[387] Um eine Eintrittskarte zu einem Spiel zu erhalten, war es nötig, sich mit detaillierten Personalauskünften um die Karte zu bewerben. Die Daten der Personen, die schließlich ein Ticket erwarben, wurden in einer Datenbank gespeichert. Auf den Tickets selbst wurde ein Chip mit einer individuellen Seriennummer angebracht und die Nummern den entsprechenden Personen der Datenbank zugeordnet. Am Eingang der Stadien befanden sich Lesegeräte, die die Seriennummer des Chips erfassten. So konnten die personenbezogenen Daten aus der Datenbank mit der Seriennummer verglichen werden.

Neben den gerade genannten Beispielen, die bereits umsetzbare oder umgesetzte Anwendungen der RFID-Technologie darstellten, sind auch Einsatzfelder des Ubiquitären Computing denkbar, die zukünftig Realität werden könnten. Eines davon ist das Gesundheitswesen.[388] Hier kann das Ubiquitäre Computing in verschiedenen Bereichen,

---

[385] Hierzu siehe *Holznagel/Bonnekoh*, MMR 2006, 17 (18).

[386] *Bundesministerium für Bildung und Forschung [Hrsg.]*, TAUCIS. Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung, 2006, S. 56.

[387] Ausführlich hierzu siehe *Conrad*, CR 2005, 537-544.

[388] Ausführlich hierzu siehe BT-Drs. 17/405, S. 80-91.

beispielsweise in medizinischen Einrichtungen oder bei medizintechnischen Geräten, unterstützend angewandt werden. Auch ein Einsatz im häuslichen Bereich ist denkbar. Dieser könnte wie folgt aussehen. Ein Patient, der zwar krank ist, aber keiner stationären Behandlung bedarf, wird beispielsweise an Kleidung oder Schmuckstücken, mit Sensoren ausgestattet. Diese messen die Körperfunktionen wie Atmung, Herzfrequenz, Blutdruck, Sauerstoffsättigung aber auch die physischen Aktivitäten des Kranken und speichern die gewonnenen Daten. Zudem werden im Haus weitere Sensoren verteilt, die ein Bewegungsmuster des Patienten erstellen. Alle Sensoren sind miteinander und mit dem Internet verbunden und können untereinander kommunizieren. Auf diese Weise können die gesammelten Informationen ausgewertet werden. Ändern sich beispielsweise Atmung und Herzfrequenz, so kann unter Einbeziehung der Sensoren zum Bewegungsmuster und zu den physischen Aktivitäten festgestellt werden, ob die Ursache für diese Änderung in einer körperlichen Aktivität oder in einem medizinischen Notfall liegen. Wird ein Notfall registriert, so kann über die Kommunikationsnetze sofort ein Notruf ausgelöst und dem Notrufempfänger die Situation exakt dargestellt werden. Dem Patienten kann damit innerhalb kürzester Zeit geholfen werden. Wenn ein solches System des Ubiquitären Computings in Zukunft tatsächlich realisiert werden kann, würde dies die medizinische Überwachung von Patienten im häuslichen Bereich erheblich erleichtern.

### *IV. Datenschutzrechtliche Bewertung*

Im Ubiquitären Computing werden alle Lebensbereiche von Informations- und Kommunikationstechnik durchzogen. Diese Allgegenwärtigkeit der Datenverarbeitung kann vor allem in datenschutzrechtlicher Hinsicht zu Schwierigkeiten führen.

Da viele Dinge, die das Alltagsleben der Menschen berühren, miteinander vernetzt sind, automatisch miteinander kommunizieren und Daten austauschen, besteht die Gefahr des Datenmissbrauchs. Dieser Missbrauch kann zum einen durch die Anbieter der Systeme selbst geschehen.[389] Aufgrund der Tatsache, dass im Ubiquitären Computing eine Person beinahe überall und jederzeit von einer Technik umgeben ist, die Daten, die in irgendeinem Zusammenhang mit dieser Person stehen, sammelt, speichert und auswertet, gelangen die Anbieter an eine große Fülle an Daten. Mit diesen wäre es möglich, genaue Profile über die Nutzer der Systeme zu erstellen. Bewegungen, soziale Beziehungen und auch Präferenzen in der realen Welt könnten anhand der gesammelten Daten festgestellt und so eine Überwachungsinfrastruktur aufgebaut werden.[390] Aber nicht nur Betreiber von Ubiquitären Computing Systemen können gesammelte Daten für ihre Zwecke missbräuchlich verwenden. Auch Dritte können eine Gefahr für die Datensi-

[389] Vgl. hierzu: *Roßnagel*, MMR 2005, 71 (72).
[390] *Roßnagel*, MMR 2005, 71 (72).

cherheit darstellen.[391] So besteht die Möglichkeit durch das Abhören der Kommunikation der einzelnen Komponenten eines Systems, beispielsweise die Funksignale in einem RFID-System zwischen einem Transponder und einem Lesegerät, die gesendeten Daten abzufangen. Auch könnte der Datenaustausch gestört oder die gespeicherten Daten durch einen unbefugten Zugriff verändert werden.

Um Gefahren des Datenmissbrauchs zu bekämpfen, gibt es im deutschen Recht vor allem das Bundesdatenschutzgesetz (BDSG). Dessen Ziel ist nach § 1 Abs. 1 BDSG der Schutz des Einzelnen vor einer Beeinträchtigung seines Persönlichkeitsrechtes durch den Umgang mit seinen personenbezogenen Daten. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG alle Einzelangeben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Diese Voraussetzung für die Anwendbarkeit des BDSG kann im Ubiquitären Computing im Einzelfall problematisch sein, etwa wenn auf RFID-Chips lediglich eine Identifikationsnummer gespeichert ist, die nicht mit personalisierten Informationen verknüpft wird.[392] Deshalb müssen bei einer datenschutzrechtlichen Prüfung im Rahmen des Ubiquitären Computing immer die Voraussetzungen für die Anwendbarkeit des Datenschutzgesetzes überprüft werden.

Wie bereits erläutert soll mit den Vorschriften des BDSG das Persönlichkeitsrecht der Betroffenen geschützt werden. Der Terminus des Persönlichkeitsrechtes kann in diesem Zusammenhang mit dem vom Bundesverfassungsgericht so genannten Volkszählungsurteil[393] geprägten Begriff des Rechts auf informationelle Selbstbestimmung gleichgesetzt werden.[394] Nach dieser Entscheidung des Bundesverfassungsgerichts wird das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet und gibt dem Einzelnen das Recht über die Sammlung und Verwendung seiner persönlichen Daten selbst zu bestimmen.[395]

Um dieses Recht zu gewährleisten, kennt das deutsche Datenschutzrecht eine Reihe von Prinzipien, die bei der Auslegung der gesetzlichen Regelungen als Richtlinie dienen sollen. Diese Grundsätze sollten auch, sofern das BDSG anwendbar ist, im Bereich des Ubiquitären Computing Beachtung finden. Als ein wichtiges Prinzip ist zunächst das Verbot mit Erlaubnisvorbehalt zu nennen. Dieses ist in § 4 Abs. 1 BDSG gesetzlich festgeschrieben. Danach ist die Erhebung, Verarbeitung oder Nutzung personenbezoge-

[391] Ausführlich zu der im Folgenden beschriebenen Gefährdung der Datensicherheit in Bezug auf die RFID-Technologie: *Holznagel/Bonnekoh*, in: Bullinger/ten Hompel, Internet der Dinge, 2007, S. 387ff; *Holznagel/Bonnekoh*, MMR 2006, 17 (22).

[392] BT-Drs. 17/405, S. 108.

[393] BVerfGE 65, 1 = NJW 1984, 419.

[394] *Gola/Schomerus*, BDSG, 9. Aufl. (2007), § 1 Rn. 6.

[395] BVerfGE 65, 1 (43).

ner Daten nur zulässig, soweit dies das BDSG oder sonstige Rechtsvorschriften es erlauben oder der Betroffene einwilligt. Im BDSG finden sich verschiedene Tatbestände, welche den Umgang mit Daten zulassen. Sie müssen danach unterschieden werden, welche Stellen die Datenverarbeitung vornehmen. Werden die Daten durch öffentliche Stellen erhoben, verarbeitet oder genutzt, so kann dies in zulässiger Weise vor allem nach den §§ 14, 15, 16 BDSG geschehen. Nicht-öffentliche Stellen oder öffentlich-rechtliche Wettbewerbsunternehmen kann dagegen die Datenverarbeitung insbesondere nach §§ 28 - 30, 32, 35 BDSG erlaubt sein. Findet sich kein gesetzlicher Erlaubnistatbestand, so kann die Nutzung der Daten auch durch eine Einwilligung, das heißt eine vorherige Einverständniserklärung, zulässig sein.[396] Kann eine Erlaubnis weder von gesetzlichen Regelungen, noch von einer Einwilligung hergeleitet werden, so ist die Nutzung der Daten verboten. Dieses Prinzip kann in der Praxis des Ubiquitären Computing zu Problemen führen. Aufgrund der Vielzahl unterschiedlicher Abläufe, die der Nutzer eines Systems ständig ausgesetzt ist, ist das Erfordernis einer Einwilligung impraktikabel.[397] Für jede Datenverarbeitung eine gesonderte Einwilligung einzufordern bzw. abzugeben wird kaum möglich sein. Das Verbot mit Erlaubnisvorbehalt in seiner jetzigen Ausprägung steht daher in einem Spannungsverhältnis zu einer effektiven Umsetzung des Ubiquitären Computings.

Ein weiterer Grundsatz, der dem deutschen Datenschutzrecht zugrunde liegt, ist das so genannte Transparenzgebot.[398] Nur wenn dem Einzelnen bekannt ist, wann welche Informationen über ihn erhoben und gespeichert werden, kann er selbstbestimmt über die Verwendung seiner Daten entscheiden.[399] Erst durch die Offenlegung wird dem Betroffenen die Möglichkeit gegeben, Korrektur-, Löschungs- oder Schadensersatzansprüche aus dem BDSG geltend zu machen und so sein Recht auf informationelle Selbstbestimmung wahrnehmen.[400] Im Bundesdatenschutzgesetz schlägt sich das Transparenzgebot in zahlreichen Vorschriften nieder, wie beispielsweise den Auskunftsrechten nach §§ 19 und 34 sowie den Benachrichtigungspflichten nach §§ 19a und 33. Aber auch dieses Prinzip kann im Ubiquitären Computing zu Problemen führen. Ähnlich wie auch bei dem Erfordernis der Einwilligung führt die Allgegenwärtigkeit der Informationstechnik zu Schwierigkeiten bei der Einhaltung des Transparenzgebotes.[401] Würde jede Datenverarbeitung im Ubiquitären Computing dem Nutzer transparent gemacht, so bestünde die Gefahr, dass der Betroffene alleine aufgrund der großen Fülle an Benachrichtigungen unaufmerksam wird und damit dem Ziel des Transparentgebotes, eine selbst-

[396] *Gola/Schomerus*, BDSG, 9. Aufl. (2007), § 4 Rn. 15f.
[397] *Roßnagel/Müller*, CR 2004, 625 (629 f.).
[398] Ausführlich siehe: *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 136.
[399] Vgl. BVerfGE 65, 1 (43).
[400] *Gola/Schomerus*, BDSG, 9. Aufl. (2007), § 33 Rn. 1.
[401] *Roßnagel/Müller*, CR 2004, 625 (628 f.).

bestimmte Entscheidung über die eigenen Daten zu ermöglichen, entgegengewirkt würde. Ein weiterer Konflikt ergibt sich aus der Tatsache, dass Systeme des Ubiquitären Computing gerade darauf abzielen, den Nutzer möglichst unmerklich im Alltag zu unterstützen. Bei einer ständigen Unterrichtung über die Datenverarbeitung ist eine solche unauffällige Vorgehensweise kaum noch möglich.

Ebenfalls ein Prinzip des deutschen Datenschutzrechtes ist der Grundsatz der Zweckbindung. Er ist nicht ausdrücklich in den Vorschriften des BDSG geregelt, liegt aber vielen Normen als Leitprinzip zugrunde.[402] Der Grundsatz besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nur gemäß dieser Zwecke verarbeitet werden dürfen.[403] Die Festlegung der Zwecke muss dabei bereits vor Erhebung der Daten erfolgt sein.[404] Eine nachträgliche Änderung des Zwecks ist nur in den gesetzlich vorgesehenen Fällen, beispielsweise nach § 14 Abs. 2 BDSG, möglich und fällt ebenfalls unter das bereits angesprochene Verbot mit Erlaubnisvorbehalt.[405] Das heißt, dass jede Änderung des Zwecks der Datenerhebung und Verarbeitung den betroffenen Personen angezeigt werden muss. Im Ubiquitären Computing soll der Nutzer durch angebotene Dienste in seinem Alltag unterstützt werden. Dazu ist es notwendig, dass die Systeme fortwährend Daten erheben, die verschiedenen Komponenten in einem System kommunizieren und dann entsprechend dem gezeigten Verhalten des Nutzers spontan reagieren und ihre Dienstleistungen anbieten.[406] Damit liegt aber bei Erhebung der Daten noch kein konkreter Zweck vor. Dieser wird vielmehr erst als Reaktion auf die Verhaltensweisen des Nutzers festgelegt. Der Grundsatz der Zweckbindung steht also im Widerspruch zu einem Grundgedanken des Ubiquitären Computing.[407]

Eng verknüpft mit dem Grundsatz der Zweckbindung ist der Erforderlichkeitsgrundsatz. Nach diesem dürfen personenbezogene Daten nur erhoben und verarbeitet werden, soweit es für die Erreichung des festgesetzten Zweckes erforderlich ist.[408] Für nichtöffentliche Stellen hat dieses Prinzip unter anderem in § 28 Abs. 1 S. 1 Nr. 1 BDSG Eingang gefunden. Nach dieser Norm darf die Erhebung und Verarbeitung der Daten nur geschehen, wenn dies zur Begründung, Durchführung oder Beendigung eines Schuldverhältnisses mit dem Betroffenen erforderlich ist. Aufgrund seiner Ausrichtung

[402] So beispielsweise § 14 Abs. 1 BDSG, wonach öffentliche Stellen eine Datenverarbeitung nur vornehmen dürfen, wenn es zur Erfüllung ihrer Aufgaben erforderlich ist und die Verarbeitung für die Zwecke erfolgt, für die die Daten erhoben worden sind.

[403] *Holznagel/Bonnekoh*, in: Bullinger/ten Hompel, Internet der Dinge, 2007, S. 373.

[404] *Gola/Schomerus*, BDSG, 9. Aufl. (2007), § 14 Rn. 9.

[405] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 135.

[406] Ähnlich auch: BT-Drs. 17/405, S. 110.

[407] BT-Drs. 17/405, S. 110.

[408] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 135f.

am Zweck der Datenerhebung ergeben sich im Hinblick auf den Erforderlichkeitsgrundsatz die gleichen Konflikte mit dem Ubiquitären Computing wie hinsichtlich des Grundsatzes der Zweckmäßigkeit.[409] Ist schon der Zweck vor Erhebung der Daten unklar, so ist eine Entscheidung, welche Datennutzung zur Erreichung des Zwecks erforderlich ist, nicht möglich.

Konkretisiert wird der Erforderlichkeitsgrundsatz durch den Grundsatz der Datensparsamkeit.[410] Dieser ist in § 3a BDSG gesetzlich festgeschrieben. Danach muss die Erhebung, Verarbeitung und Nutzung personenbezogener Daten an dem Ziel ausgerichtet sein, so wenige Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere muss dabei eine Anonymisierung und Pseudonymisierung der Daten erfolgen, soweit dies nach dem Verwendungszweck möglich ist und keinen unverhältnismäßigen Aufwand erfordert. Im Ubiquitären Computing wird eine Vielzahl von Daten gesammelt und verarbeitet, um eine passende Reaktion auf das Verhalten des Nutzers finden zu können. Hierdurch besteht die Gefahr, dass sehr viele personenbezogene Daten erhoben werden. Allerdings bietet sich für die Anbieter von Systemen des Ubiquitären Computing die in § 3a S. 2 BDSG vorgesehene Anonymisierung und Pseudonymisierung der Daten an. So kann auch im Ubiquitären Computing dem gesetzlichen Gebot der Datensparsamkeit genügt werden.

### *V. Fazit*

Das Ubiquitäre Computing als allgegenwärtige Vernetzung von Computerleistung und Informationstechnologie ist noch eine Zukunftsversion. Bisher existieren verschiedene Systeme mit unterschiedlichen Technologien, wie RFID-Systeme, Sensornetze oder Location-based Services, die jedoch noch nicht den gesamten Alltag der Menschen durchdringen. Wenn eine Welt des Ubiquitären Computings Wirklichkeit wird, dann können aus datenschutzrechtlicher Sicht Probleme auftreten. Vor allem die verschiedenen Prinzipien, die die Verwirklichung des Rechts auf informationelle Selbstbestimmung gewährleisten sollen, können mit den Grundgedanken des Ubiquitären Computing im Widerspruch stehen. Diese zu lösen wird eine Aufgabe für die Zukunft sein.

[409] *Roßnagel/Müller* CR 2004, 625 (631).
[410] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 137f.

# Kapitel 7: Augmented Reality

*P. Thal*

## *I. Begriff und Technologie*

Mediziner, Ingenieure und Architekten bilden wohl die Berufsgruppen, die am ehesten etwas mit dem Begriff der Augmented Reality (AR) anfangen können. Denn schließlich haben dort die Methoden der AR schon Einzug in den Alltag gefunden: So werden z.B. dem Chirurgen während einer Operation auf dem Operationsbildschirm bestimmte Arterien oder Venen mit Beschriftung und Lage im Körper angezeigt. Dem Fahrzeugingenieur bieten sich völlig neue Design- und Entwicklungsmöglichkeiten, wenn fahrzeuginterne Funktionen wie das Navigationssystem mit der äußeren Umgebung (z.B. Straßenverlauf) verknüpft werden können. Der Fahrer muss dann seinen Blick nicht mehr von der Straße auf das Navigationssystem und zurück wenden, damit er weiß, wo er hinfahren muss. Auf der Frontscheibe des KFZ können Hervorhebungen und Markierungen die Realität derart verändern, dass die befahrene Straße vom Fahrer nicht mehr als gewöhnliche graue Autobahn, sondern als die ins Navigationssystem eingegebene, z.B. grün markierte Reiseroute wahrgenommen wird.[411] Auch bei größeren Bauvorhaben kann die AR-Technologie den Verantwortlichen unterstützen, indem sie das fertige Projekt mit virtuellen Gebäuden und Versorgungsleitungen vor dem Auge erscheinen lässt, schon bevor der erste Spatenstich gesetzt wird. Insbesondere bei großen Fabriken können durch die Verbindung von bereits bestehenden und geplanten Anlagen auf einem Bildschirm die späteren Produktionsabläufe simuliert und optimiert werden.[412] Letztlich kann die AR-Technologie aber in jedem denkbaren Bereich eingesetzt werden. Ein Beispiel das jeder kennen dürfte, sind die Markierungen die bei Sportübertragungen im Fernsehen eingeblendet werden, um z.B. zu zeigen wie weit die Mauer aus Abwehrspielern vom Freistoßpunkt entfernt sein muss oder wie viele Yards das Football-Team noch zu bewältigen hat.

Der Begriff Augmented Reality kann ins Deutsche als „erweiterte Realität“ übersetzt werden und beschreibt die computergestützte Erweiterung der Realitätswahrnehmung. In den allermeisten Fällen geschieht dies durch veränderte visuelle Wahrnehmung der Wirklichkeit, wobei eine Beschränkung nur auf diese Sinneswahrnehmung freilich nicht besteht. Voraussetzung für eine veränderte Wahrnehmung ist somit regelmäßig ein Bildschirm oder ein anderes bilddarstellendes Medium (wie z.B. Display-Brillen)[413],

[411] Siehe zur AR im Bereich des Ingenieurwesens: *Tönnies,* Towards augmented reality, S. 2 ff.
[412] *Pentenrieder,* Augmented Reality based Factory Planning, S. 3 ff.
[413] Display-Brillen gibt es mittlerweile auch schon für den Endverbraucher, so z.B. die „Transcend Ski

mithilfe dessen bestimmte Eigenschaften der Realität hinzugefügt oder ausgeblendet werden können. Sogenannte Eye-Tracker können die Bedienung von AR-Endgeräten erleichtern, indem sie die Blickbewegungen des Nutzers identifizieren und die angezeigten Elemente auf dem Bildschirm entsprechend anpassen. Die Ergonomie der Endgeräte wird dabei auch immer weiter entwickelt, sodass mittlerweile auch schon Mobiltelefone die AR-Technologie nutzen können. Die sogenannten Reality-Browser[414] ermöglichen es dem User, bestimmte Orte wie z.B. Restaurants auf dem Bildschirm, den seine Handykamera „live" aufnimmt, anzeigen zu lassen. Eine audiovisuelle Anwendung der AR-Technologie könnte z.B. darin bestehen, dass man mit seiner Handykamera eine Oper oder einen Konzertsaal aufnimmt und über die Lautsprecher hören kann, welches Stück gerade gespielt wird.

### *II. Rechtliche Bewertung*

#### *1. Allgemeines*

Fraglich ist, ob es überhaupt AR-spezifische Rechtsprobleme gibt. Denn insoweit liegt es hier wie bei vielen neuen IT-Phänomenen: Klassische Straftatbestände wie die Beleidigung oder der Betrug können freilich auch im neuen Gewand der modernen Technologie begangen werden. Damit liegt aber nur eine neue Begehungsweise und eben kein AR-spezifisches Rechtsproblem vor. Wird z.B. eine Person von einem Reality-Browser erfasst und mit der Eigenschaft „schlechter Liebhaber" oder „vorbestrafter Sexualverbrecher" versehen, kommt eine Strafbarkeit wegen §§ 185 ff. StGB in Betracht, ohne dass ein Tatbestandsmerkmal der Vorschriften besonders ausgelegt oder angewendet werden muss. Gleiches gilt für den Fall, in dem ein AR-Dienst für Mobiltelefone einen Kunden unter Angabe falscher Angebote in bestimmte Kaufhäuser lockt oder von bestimmten konkurrierenden Kaufhäusern fernhalten will. Die damit verbundene Täuschungshandlung des AR-Dienstbetreibers ruft einen Irrtum beim User hervor, der letztlich dazu führen soll, dass ein Dritter oder der Betreiber selbst einen Vermögensvorteil erhält. § 263 StGB käme mithin in Betracht. Auch die computerstrafrechtlichen Vorschriften der §§ 202a ff. StGB und §§ 303a f. StGB sind typischerweise dort relevant, wo Daten fließen und ausgetauscht werden, zumal dies bei der AR-Technologie meist drahtlos erfolgt.[415]

#### *2. Elektronisches Graffiti - § 303 Abs. 2 StGB?*

Fraglich ist aber, ob sich aus § 303 Abs. 2 StGB ein anderes ergibt. Dazu folgender

---

Goggles Feature Cyborg HUD" von ZealOptics.

[414] Z.B. Layar Reality Browser.

[415] Siehe zu den §§ 202a ff. StGB im Bereich des WLAN *Thal* in *Hilgendorf*, Dimensionen des IT-Rechts, S. 43, 52 ff.

Fall: A bietet eine Augmented Reality-App für mobile Endgeräte an. Der Dienst zeigt seinen Usern mithilfe der Handykamera die „besten Locations der Stadt“ (Bars, Restaurants, Museen) dergestalt an, dass die Gebäude, in denen sich die Örtlichkeiten befinden, auf dem Display rot schraffiert erscheinen. Weil A aber die städtischen Denkmäler und Kirchen nicht leiden kann, hat er die App so programmiert, dass diese Orte völlig zerstört und verwüstet aussehen, wenn man die Kamera der Endgeräte davor hält. Dies alles funktioniert in Echtzeit, d.h. dem User wird über die Handykamera „live“ die Umgebung mit den entsprechenden Änderungen angezeigt, ohne dass die Bilder der Locations oder Kirchen extra geladen werden müssen. Strafbarkeit des A nach § 303 Abs. 2 StGB?

*a) Fremde Sache*

Nach § 303 Abs. 2 StGB wird bestraft, wer unbefugt das Erscheinungsbild einer fremden Sache nicht nur unerheblich und nicht nur vorrübergehend verändert. Als taugliches Tatobjekt muss zunächst eine „fremde Sache“ vorliegen. Bei § 303 Abs. 2 StGB gelten insoweit die gleichen Grundsätze wie bei § 303 Abs. 1 StGB, sodass anders als bei den §§ 242 ff. StGB auch unbewegliche Sachen wie Gebäude oder Ruinen erfasst sind. Vorliegend geht es im Fall um Gebäude und Kirchen, sodass sowohl die Fremdheit als auch die Gegenständlichkeit bejaht werden können. Fraglich ist aber, ob schon an dieser Stelle diskutiert werden muss, dass der A vorliegend wohl nicht das Gebäude selbst, sondern nur die Daten ändert, die das Objektiv der Handykamera liefert. Denn insoweit sind Daten regelmäßig keine Sachen im Sinne des § 303 Abs. 2 StGB, sodass höchstens § 303a StGB in Betracht käme. Nachdem aber bei § 303 Abs. 2 StGB das Tatobjekt durch das „Erscheinungsbild“ noch weiter konkretisiert wird, empfiehlt sich die Diskussion unter diesem Prüfungspunkt.

*b) Äußeres Erscheinungsbild*

*aa) Allgemeines*

Die fremde Sache interessiert nur hinsichtlich ihres Erscheinungsbildes.[416] Das äußere Erscheinungsbild einer Sache wird bestimmt durch ihre Form, ihre Oberfläche, aber auch durch ihre Umgebung.[417] Die Begründung des 39. StrÄndG zeigt, dass der Begriff Erscheinungsbild weit aufgefasst worden ist und nicht nur auf Änderungen von Form und Oberfläche der Sache selbst beschränkt werden sollte.[418]

In der Literatur wird die Frage nach der Unmittelbarkeit der Einwirkung auf die Sache selbst uneinheitlich beantwortet. Während manche von einem engen Verständnis

[416] LK/*Wolff*, § 303 Rn. 28.
[417] LK/*Wolff,* § 303 Rn. 28.
[418] BT-Drs. 15/5313, S. 3; *Fischer,* StGB, § 303 Rn. 18; LK/*Wolff,* § 303 Rn. 28.

des „Veränderns des Erscheinungsbildes“ ausgehen und insoweit immer eine unmittelbare Einwirkung auf die Sache selbst fordern[419], sprechen sich andere Stimmen für eine grundsätzlich weite Auslegung aus und grenzen den Tatbestand erst an späterer Stelle ein.[420] Darüber hinaus finden sich auch abweichende Meinungen darüber, ob aufgrund einer engen Auslegung die Tathandlung oder das Tatobjekt des § 303 Abs. 2 StGB nicht gegeben ist.[421] Je nachdem ob man das „Erscheinungsbild“ oder das „Verändern“ konkretisieren will, ist an einem der Punkte eine Auslegung der Begriffe erforderlich.

Die Gesetzesmaterialien geben aber auf beide Probleme eine eindeutige Antwort. So heißt es in der Begründung: „Liegt keine Einwirkung auf die Sache oder den Gegenstand vor, wird in der Regel von einer nur unerheblichen, nicht dauerhaften und damit vom Tatbestand nicht erfassten Veränderung auszugehen sein.“ Eine unerhebliche Veränderung ist aber dennoch eine „Veränderung“, sodass zunächst festgehalten werden kann, dass die Einschränkung des Tatbestands nicht auf Ebene der Tathandlung geschehen soll. Eine nur mittelbare Einwirkung auf die Sache ist somit eine Veränderung im Sinne des § 303 Abs. 2 StGB. Ferner finden sich auch keine Anhaltspunkte dafür, dass das Erscheinungsbild der Sache nicht auch fernere Umstände als die Substanz bzw. Oberfläche erfasst. Vielmehr heißt es weiter: „Als Beispiele sind die Fälle zu nennen, dass Wäsche deutlich sichtbar auf dem Balkon eines Wohnhauses aufgehängt oder an der Außenfassade ein Spruchband angebracht wird, ohne die Substanz des Gebäudes zu beeinträchtigen.“ Solche Handlungen sind zwar nicht mehr vom Tatbestand erfasst, weil sie unerheblich bzw. nur vorrübergehend sind, nicht aber weil sie nicht das Erscheinungsbild der Sache betreffen. Mithin lässt sich zusammenfassen, dass auch die direkte Umgebung der Sache vom Begriff des Erscheinungsbilds erfasst ist.[422]

Die städtischen Kirchen und Denkmäler werden nicht an ihrer Oberfläche oder in ihrer Form verändert. Eine unmittelbare Einwirkung auf die Gebäude selbst liegt mithin nicht vor. Dies wäre aber unschädlich, wenn auch die Umgebung oder fernere Umstände zum Erscheinungsbild der Kirchen und Denkmäler gehören. Nach der Gesetzesbegründung zum 39. StrÄndG und Teilen der Literatur verändern auch solche Handlungen das Erscheinungsbild einer Sache, die die Sache nur mittelbar betreffen und insoweit z.B. nur ihre Umgebung umgestalten.[423] Vorliegend wird das Erscheinungsbild der Gebäude dadurch verändert, dass es für die User des AR-Dienstes auf ihrem Display an-

---

[419] *Hillenkamp,*in: FS Schwind, 2006, S. 927, 938; Schönke/Schröder/*Stree,* § 303 Rn. 9a; *Lackner/Kühl,* § 303 Rn. 7b; *Wessels/Hillenkamp*, Rn. 31b.

[420] LK/*Wolff,* § 303 Rn. 28; Kritisch, im Ergebnis aber ähnlich: *Fischer*, StGB, § 303 Rn. 18a.

[421] Tathandlung als Ansatzpunkt: *Fischer*, StGB, § 303 Rn. 18a*; Hillenkamp,*in: FS Schwind, 2006, S. 927, 938; *Lackner/Kühl,* § 303 Rn. 7b; Schönke/Schröder/*Stree,* § 303 Rn. 9a; anders: LK/*Wolff,* § 303 Rn. 28.

[422] Im Ergebnis auch: LK/*Wolff,* § 303 Rn. 28.

[423] BT-Drs. 15/5313 S. 3; LK/*Wolff,* § 303 Rn. 28.

ders erscheint als in Wirklichkeit. Dadurch wird sprichwörtlich das Bild der Kirchen, wie es nach außen in Erscheinung tritt, verändert. Der Umstand, dass das Erscheinungsbild der Kirche nur für diejenigen Personen, die den AR-Dienst nutzen, verändert ist, betrifft vielmehr die Frage nach der Erheblichkeit oder Dauer der Veränderung.

*bb) Dreifache Einschränkung?*

Will man den oben genannten Fall der Augmented-Reality schon an dieser Stelle des Tatbestands scheitern lassen, muss man das Erscheinungsbild definieren als die Oberfläche, Form, Umgebung einer Sache, *wie sie von jedermann wahrgenommen wird*. Andererseits könnte man „Erscheinungsbild einer Sache" schon begriffsnotwendig als das verstehen, was *jeder* sehen kann. Damit wären aber solche Fälle schwierig zu beurteilen, in denen z.B. erst der Einsatz von Schwarzlichtlampen dem Betrachter die Wahrnehmung des wahren Erscheinungsbilds ermöglicht. Insoweit müsste man das Erscheinungsbild dann noch auf das beschränken, was *mit bloßem Auge* sichtbar ist. Im Übrigen könnte man dahingehend argumentieren, dass im Schwarzlicht-Fall zumindest *irgendeine Sache* tatsächlich verändert wurde, wohingegen im Augmented-Reality-Fall genau genommen nur das elektronische Pendant der Kirchen und Denkmäler betroffen ist. Denn insoweit bleibt die Kirche neben der Darstellung auf dem Display völlig unberührt, wohingegen im Schwarzlicht-Fall auf die Oberfläche des konkreten Gebäudes eingewirkt wird. Eine solche Beschränkung des Begriffs „Erscheinungsbild" auf das, was *von jedermann* und *mit bloßem Auge* gesehen werden kann, findet weder in der Literatur noch in den Gesetzesbegründungen Erwähnung und soll deswegen nicht zur Begrenzung herangezogen werden. Hätte der Gesetzgeber gewollt, dass nur unmittelbare Einwirkungen auf die Sache erfasst sind, hätte der § 303 Abs. 2 StGB lauten können: „Ebenso wird bestraft, wer unbefugt *eine fremde Sache* nicht nur unerheblich und nicht nur vorrübergehend in ihrem Erscheinungsbild *verändert*". Das Erscheinungsbild der Denkmäler und Kirchen ist mithin betroffen.

*c) Verändern*

Unter Verändern im Sinne des § 303 Abs. 2 StGB versteht man jedes kausale Verhalten, dass das Erscheinungsbild der Sache umgestaltet. Dies ist beim Verändern durch den AR-Dienst gegeben.

*d) Nicht nur unerheblich und nicht nur vorrübergehend*

Der weite Tatbestand des § 303 Abs. 2 StGB soll durch das Merkmal „nicht nur unerheblich und nicht nur vorrübergehend" eingeschränkt werden.[424] Nach diesem Korrektiv sind in der Regel nur solche Veränderungen erheblich, bei denen unmittelbar auf die

[424] BT-Drs. 15/5313 S. 3; *Fischer,* StGB, § 303 Rn. 19; LK/*Wolff,* § 303 Rn. 30.

Substanz der Sache eingewirkt wird, wie dies namentlich bei Graffiti der Fall ist.[425] So soll z.B. das Aufhängen von Wäsche auf einem Balkon oder das Anbringen eines Spruchbands das Erscheinungsbild eines Gebäudes nicht erheblich verändern. Gleiches gilt für Umgestaltungen, die ohne Aufwand wieder entfernt werden können oder von alleine vergehen, wie z.B. das Bemalen wie Kreiden- oder Wasserfarbe.[426] Diese Veränderungen sind nur vorrübergehender Natur, weil ihnen entweder das zeit- oder auf die Intensität der Substanzeinwirkung bezogene Moment fehlt.[427]

Vorliegend sprechen viele Gesichtspunkte gegen die Erheblichkeit der Veränderung durch den AR-Dienst. Zum einen kann die Umgestaltung nicht von jedermann wahrgenommen werden, sondern nur von den Usern des konkreten AR-Dienstes. Ferner bleibt die eigentliche Sache völlig unberührt, weil genau genommen nur ihr elektronisches Pendant umgestaltet wird. Die von A vorgenommenen Veränderungen sind mithin nicht erheblich.

### *e) Ergebnis*

Bei unbefangener Betrachtung des obigen Falls ist es relativ eindeutig, dass es sich dabei nicht um strafwürdiges Unrecht handeln kann. Die konkrete Subsumtion hat aber gezeigt, dass der § 303 Abs. 2 StGB - mit seinem vom Gesetzgeber so vorgesehenen weiten Tatbestand – selbst höchsttechnologische Begehungsweisen erfasst und dabei neue Probleme schafft. Beinhaltet das Erscheinungsbild einer Sache schon begrifflich all das, was jedermann mit bloßem Auge sehen kann oder muss dieses Merkmal weiter verstanden werden? Obgleich die Begründung zum 39. StrÄndG relativ eindeutig von Letzterem ausgeht, bleibt es abzuwarten, wie die Rechtsprechung den Begriff konturieren wird, wenn sie das erste Mal mit elektronischem Graffiti konfrontiert wird.

---

[425] BT-Drs. 15/5313 S. 3.
[426] *Fischer,* StGB, § 303 Rn. 19; LK/*Wolff,* § 303 Rn. 30.
[427] *Wessels/Hillenkamp*, Rn. 31b.