Cloud Computing aus Sicht der Ethik

13

Oliver Bendel

Zusammenfassung

Zahlreiche Unternehmen transferieren Daten ihrer Kunden in die Cloud, oder diese werden selbst aktiv, nutzen spezielle Dienste und soziale Medien. Es stellen sich viele Fragen: Wird der Benutzer genügend informiert? Sind ihm alle Konsequenzen des Vorgangs klar? Was ist, wenn Inhalte als verdächtig angesehen und Informationen an Behörden weitergereicht werden? Wie können lebenswichtige und personenbezogene Daten geschützt werden? Der Beitrag stellt Probleme rund um Cloud Computing für Privatkunden aus Sicht des Verbraucherschutzes und der Informationsethik systematisch dar, mit Fokus auf Bild und Text. Aus der Unternehmensethik heraus werden Vorschläge für Anbieter unterbreitet.

Schlüsselwörter

Cloud Computing · Verbraucherschutz · Informationsethik · Unternehmensethik · Wirtschaftsethik · Konsumentenethik

13.1 Cloud Computing ist überall

Der Begriff der Cloud ist, wie das dazugehörige Phänomen, allgegenwärtig. Betriebe speichern ihre Daten in der Wolke, entwickeln Anwendungen in ihr und nutzen Software über sie (vgl. Bedner 2010; Münzl 2015). Je nach Anforderung werden Public, Private, Hybrid oder Community Clouds bevorzugt. Privatpersonen laden

Überarbeiteter Beitrag basierend auf Bendel (2016) Cloud Computing aus Sicht von Verbraucherschutz und Informationsethik, HMD – Praxis der Wirtschaftsinformatik Heft 311, 53(5):607–618.

O. Bendel (✉)
Fachhochschule Nordwestschweiz, Windisch, Schweiz
E-Mail: oliver.bendel@fhnw.ch

S. Reinheimer (Hrsg.), *Cloud Computing*, Edition HMD,
https://doi.org/10.1007/978-3-658-20967-4_13

ihre Fotos (z. B. Profilbilder, Party- und Urlaubsfotos) und ihre Dokumente hoch, seien es Notizen, Tagebücher oder Manuskripte. Sie machen dies absichtlich und absichtsvoll, insofern sie beim Hochladen selbst aktiv werden und ihre Gründe dafür haben, mögen diese in der Sicherheit liegen oder in der Flexibilität, oder unabsichtlich und unachtsam, insofern ihre Daten ohne ihr Wissen durch den Anbieter bzw. den Dienst und das Gerät synchronisiert werden.

Der vorliegende Beitrag diskutiert unterschiedliche Anwendungs- und Verhaltensweisen. Er zeigt, dass Cloud Computing für Privatpersonen (und Unternehmensmitarbeiter) aus Sicht von Verbraucherschutz und Informationsethik sowohl Risiken als auch Chancen beinhaltet, wobei vor allem die einen ausformuliert werden, da damit Handlungsbedarf verbunden ist, und die anderen angedeutet sind. Am Rande, soweit für die ethische Auseinandersetzung relevant, werden rechtliche Fragen angesprochen. Der Begriff des Cloud Computing wird bewusst weit gehalten, und es werden klassische Speicherdienste ebenso einbezogen wie – für Privatpersonen besonders relevant – bestimmte soziale Netzwerke und Kommunikationsdienste, über die man Inhalte hochlädt, verteilt und bewahrt.

13.2 Die verschiedenen Wolken

Wie Big Data gilt Cloud Computing als disruptiver Ansatz (vgl. Atchison et al. 2014). Dienste, Anwendungen und Ressourcen werden über Hochleistungsserver meist externer Anbieter „flexibel und skalierbar … angeboten“, und zwar „ohne eine langfristige Kapitalbindung und IT-spezifisches Know-how vorauszusetzen“ (Repschläger et al. 2010). „Es handelt sich um eine Form des IT-Sourcings, bei der der komplette Betrieb und Wartungsaufwand beim Anbieter verbleibt und ausschließlich die Leistung vom Kunden angemietet und verbrauchsabhängig bezahlt wird.“ (ebd.) Damit wird der Normalfall der Public Cloud angesprochen, bei der es eben einen externen Anbieter gibt. Auch kostenloser Gebrauch ist möglich, gerade für Privatpersonen.

Infrastructure as a Service (IaaS) ist der Zugang zu virtualisierten Hardwareressourcen, etwa Computern, Netzwerken und Speichern, Platform as a Service (PaaS) zu Programmierungs- oder Laufzeitumgebungen mit dynamisch anpassbaren Rechen- und Datenkapazitäten, Software as a Service (SaaS) zu Softwaresammlungen und Anwendungsprogrammen (vgl. Abts und Mülder 2013, S. 151 ff.). Dieser Beitrag konzentriert sich auf IaaS für Privatpersonen, insbesondere auf Speicher- und File-Sharing-Dienste für Texte und Fotos. Der Up- und Download von Musik wird, da es sich um einen eigenen großen Problembereich handelt, weitgehend ausgeklammert (vgl. Köhler 2012), ebenso die Selbstvermessung, das Quantified Self. Die Verzeichnisse sind entweder nur persönlich (und eventuell für den Anbieter) sichtbar oder aber für Freunde bzw. Gruppen oder sogar für die Weltöffentlichkeit freigegeben.

Ein Spezialfall sind Private Clouds, bei denen sich Anbieter und Nutzer im selben Unternehmen befinden bzw. Privatpersonen ihre eigenen Dienste betreiben. Immer häufiger werden Public Cloud und Private Cloud zusammengeführt zur

Hybrid Cloud. Beispielsweise werden streng vertrauliche Dokumente in der Private Cloud untergebracht, weniger vertrauliche und massenhaft anfallende Daten dagegen in der Public Cloud. Im gegebenen Kontext interessiert vor allem die Public Cloud, bei der rechtliche und ethische Fragen unmittelbar auftauchen und die für Privatpersonen der übliche Anwendungsfall ist. Natürlich sind auch Private Clouds nicht vor Missbrauch geschützt, und Hybrid Clouds können entsprechende Lücken aufweisen, ebenso die hier nicht weiter thematisierten Community Clouds.

13.3 Verbraucherschutz und Informationsethik

Verbraucherschutz, auch Konsumentenschutz genannt, ist der Schutz von Verbrauchern vor überteuerten, gefährlichen, schadhaften, ungeeigneten oder unnötigen Produkten und Dienstleistungen und vor Undurchschaubarkeit und Fehlinformation auf Seiten der Hersteller und Händler. Ausgangspunkt ist die Tatsache, dass Konsumenten auf die Angebote und damit auf die Firmen mehr oder weniger angewiesen sind. Sogenannte Verbraucherzentralen bieten Beratung und Informationen zu Fragen des Verbraucherschutzes, helfen bei rechtlichen Problemen, zeigen moralische Herausforderungen auf (womit Beziehungen zur Ethik entstehen) und vertreten die Interessen der Kunden und Konsumenten (vgl. Bendel 2012a). Sie sind unabhängig, überwiegend öffentlich finanziert und gemeinnützig.

Die Bereichsethik der Informationsethik hat die Moral (in) der Informationsgesellschaft zum Gegenstand. Sie untersucht, wie sich deren Mitglieder in moralischer Hinsicht verhalten respektive verhalten sollen; ebenso betrachtet sie unter sittlichen Gesichtspunkten das Verhältnis der Informationsgesellschaft zu sich selbst, auch zu nicht technikaffinen Mitgliedern, und zu wenig technisierten Kulturen (vgl. Bendel 2012b). Die Wirtschaftsethik (ebenfalls eine Bereichsethik) hat die Moral der und in der Wirtschaft zum Gegenstand. Moralische Akteure sind einzelne Menschen, die wirtschaftliche Interessen haben, die produzieren, handeln, führen und ausführen (Individualethik) sowie konsumieren (Konsumentenethik), und das Unternehmen (Unternehmensethik als Hauptgebiet der Institutionenethik), das Verantwortung gegenüber Mitarbeitern, Kunden und Umwelt trägt (vgl. Bendel 2016, S. 245; Noll 2013).

Bei der im vorliegenden Beitrag begonnenen Diskussion sind nicht nur Begriffe der Wirtschaftsethik (vor allem der Unternehmens- und der Konsumentenethik), sondern auch und vor allem der Informationsethik anzuwenden, z. B. „informationelle Autonomie“ bzw. „informationelle Selbstbestimmung“ (womit der Schwerpunkt mehr auf die Selbstbestimmung, weniger auf die Unabhängigkeit, gelegt bzw. die rechtliche Dimension mit angesprochen wird), „digitaler Graben“ und „Informationsgerechtigkeit“ (vgl. Bendel 2016), zudem „digitale Identität“. Informationelle Autonomie ist die Möglichkeit, unabhängig und selbstständig auf Informationen zuzugreifen, über die Verbreitung von eigenen Äußerungen und Abbildungen selbst zu bestimmen sowie die Daten zur eigenen Person einzusehen und gegebenenfalls anzupassen (vgl. ebd., S. 11 f.). Der digitale Graben verläuft zwischen schwach und stark vernetzten und computerisierten Ländern sowie innerhalb der Informationsgesellschaft und trennt diejenigen, die

Zugang zum Internet und zu Onlinediensten haben, von denjenigen, die ihn nicht haben oder nicht haben wollen (vgl. ebd., S. 47). In der Tendenz widerspricht der digitale Graben dem Gerechtigkeitsprinzip (vgl. Kuhlen 2004). Die Informationsgerechtigkeit bezieht sich auf den der Allgemeinheit möglichen Zugang zur Information und zu IKT und ist mit der Informationsfreiheit (d.i. Informationszugangsfreiheit) verbunden. Die digitale Identität bildet sich im Netz ausgehend von einem Profil und die Aktivitäten des Benutzers über eine Zeitspanne dokumentierend. Sie ist auch im realen Raum (etwa bei der Jobsuche und im Freundeskreis) von großer Bedeutung und eine feste Referenzgröße. Mehr und mehr gibt es zusätzlich zu der digitalen Identität, die vom Benutzer generiert wird, digitale Identitäten, die von Behörden und Unternehmen erstellt und gepflegt werden.

13.4 Das unbeabsichtigte vs. das beabsichtigte Hochladen

Dem Anwender ist in einem gewissen Umfang zuzumuten, sich mit Blick auf Cloud-Dienste, App-Einstellungen und Endgeräte zu informieren. Allerdings kann es vorkommen, dass er aufgrund mangelnder Bildung respektive Vorstellungskraft oder von Einschränkungen nicht in der Lage dazu ist. Die Ursache des Informationsdefizits liegt in diesen Fällen offenbar bei ihm. Wenn der Benutzer, der sich in diesem Sinne nicht auf einen adäquaten Stand bringen konnte, das erfolgte Hochladen nicht aktiv initiiert oder nicht intendiert hat, wird anscheinend gegen seine informationelle Selbstbestimmung verstoßen. Man kann freilich argumentieren, dass Selbstbestimmung eben die Bestimmung durch das Selbst ist, und wenn diese aus Gründen, die im Selbst liegen, nicht erfolgen kann, habe man das Recht darauf verwirkt.

Ein häufiges Phänomen ist indes, dass der Benutzer einen Vorgang gar nicht verstehen kann, weil der Cloud-Anbieter sich nicht klar und deutlich ausdrückt, oder jenem nicht zuzumuten ist, den Vorgang zu durchleuchten, weil die Erklärungen und Bestimmungen mehrere Seiten umfassen oder in einer ihm nicht zugänglichen Sprache wie Englisch verfasst sind. Die Ursache des Problems liegt hier zweifelsohne beim Unternehmen. Nicht zuletzt mag dieses mit technischen oder medialen Anforderungen aufwarten, denen der Benutzer nicht entsprechen kann, z. B. weil er zu bestimmten Instrumenten oder Diensten keinen Zugang hat oder sich Versionen, Updates und Upgrades nicht leisten kann, etwa bei Betriebssystemen und Anwendungsprogrammen. Die informationelle Selbstbestimmung scheint durch das absichtliche oder unabsichtliche, immerhin aber in Kauf genommene Aufstellen von informationellen Hindernissen oder Ausheben eines digitalen Grabens verletzt zu werden.

Der beabsichtigte Upload scheint vorderhand unproblematisch zu sein. Der Benutzer hat beispielsweise erklärt, die AGB gelesen und verstanden zu haben (oft im Widerspruch zur Realität), oder den Vorgang aktiv begonnen. Allerdings ist bei Kindern und Jugendlichen eine eingeschränkte Geschäftsfähigkeit – das wäre die rechtliche Dimension – und auch Einsichtsfähigkeit – damit kommt die moralische Perspektive ins Spiel – vorhanden. Zudem ist zu bedenken, dass sich Moral nicht nur auf andere Menschen und auf die Umwelt (einschließlich der Tiere),

sondern ebenso auf die handelnde Person selbst richten kann: Diese soll auch gut zu sich selbst sein. Die Frage ist demnach, ob der Benutzer die Konsequenzen seines Handelns voraussehen und beurteilen kann. Womöglich schadet er durch das Hochladen seinem jetzigen oder späteren Selbst, z. B. durch kompromittierende Selfies. Nun ist es nicht unbedingt Aufgabe der Firmen, den Benutzer vor sich selbst zu schützen. Es wäre aber wünschenswert, wenn Wirtschaft, Politik, Gesundheits- und Bildungswesen und Einrichtungen der Gesellschaft – einschließlich der Verbraucherzentralen – zur Aufklärung beitragen und vor zu erwartenden Konsequenzen warnen würden.

13.5 Der Content in der Cloud

13.5.1 Selbst erstellte Inhalte

Das Hochladen von selbst erstellten Inhalten (von User-generated Content im wörtlichen und unmittelbaren Sinne) ist zunächst in dem Sinne unheikel, als dem Urheberrecht entsprochen wird (vgl. Rohrlich 2013). Ein selbst verfasstes Gedicht oder ein Selbstbildnis des Benutzers landet in der Cloud und wird dort vorgehalten. Es ist der Urheber selbst, der sein Werk ausliefert. Problematisch wird es, wenn der Anbieter exklusive oder nichtexklusive Lizenzen erwirbt. Insbesondere bei sozialen Medien wie Twitter und Facebook, die als Cloud-Dienste fungieren können, ist der zweitere Fall üblich. Dadurch werden zumindest Nutzungs- und Vervielfältigungsrechte (als Dimensionen im Verwertungsrecht) eingeräumt. Beispielsweise kann ein Foto des Mitglieds (sogar eines, das es selbst zeigt) auf eine Karte oder eine Tasse gedruckt und verkauft werden. Weiter kann ein Anbieter oder ein anderer Benutzer behaupten, der Urheber zu sein, was auf eine aufwändige Klärung der wahren Verhältnisse, auch vor Gericht, hinauslaufen wird. Möglich ist daneben der Diebstahl geistigen Eigentums durch Dienst- und Plattformbetreiber oder andere Benutzer. Diese lassen sich von Fotos, Texten oder Songs inspirieren bzw. kopieren und verbreiten diese gesamthaft oder teilweise, ohne die Quelle anzugeben. Daraus resultieren nicht zuletzt moralische Probleme, etwa hinsichtlich der digitalen Identität.

13.5.2 Nicht selbst erstellte Inhalte

Das Hochladen von nicht selbst erstellten Inhalten kann aus rechtlichen Gründen problematisch sein. In vielen Ländern gilt die Datei in der Cloud als erlaubte private Kopie (vgl. Rohrlich 2013). Ist der Dienst allerdings für andere Personen oder sogar für größere Gruppen (in Deutschland von mehr als sieben Personen) oder die ganze Welt zugreifbar, wie es bei Bildplattformen wie Flickr nicht unüblich ist, handelt es sich in der Regel um eine unerlaubte Veröffentlichung und mithin eine Zuwiderhandlung mit Blick auf Urheber- bzw. Verwertungsrecht (vgl. *ebd.*). Daneben können allgemeine oder besondere Persönlichkeitsrechte tangiert sein. Ferner ist selbst bei einem kleinen Kreis die Gefahr nicht von der Hand zu weisen, dass ein

Zugehöriger seinen Zugang missbraucht und Kopien, etwa von Dokumenten, für einen großen Kreis erstellt, ohne dass dies vom Benutzer gewünscht ist und verhindert werden kann. Dabei entstehen neben rechtlichen Problemen auch moralische Herausforderungen, etwa der Verlust von Vertrauen und die Einbuße von Kontrolle über die digitale Identität, wenn personenbezogene Daten betroffen sind.

13.5.3 Inhalte mit Daten anderer Personen

Das Hochladen von Inhalten mit Daten anderer Personen kann ebenfalls rechtlich und moralisch beanstandet werden. Es kann gegen Urheber- und speziell Verwertungsrecht sowie das Persönlichkeitsrecht verstoßen. Häufig werden Kontaktdaten aus Notebooks und Smartphones von sozialen Netzwerken und Kommunikationsdiensten wie Facebook und WhatsApp abgezogen und von diesen verwendet. Unbeteiligte werden zum Zwecke der Anwerbung kontaktiert. Zudem kann das Recht am eigenen Bild berührt sein. Ein Benutzer, der ein Foto oder Video von Personen angefertigt hat, die klar und deutlich zu erkennen sind und nicht in die Veröffentlichung einwilligen, ist der Urheber, darf aber die Verwertung nicht vornehmen, da er nicht über dieses spezielle Motiv, die jeweils abgebildete Person, verfügen darf. Der Betroffene ist nicht nur im Allgemeinen in seiner informationellen Autonomie angetastet, sondern eventuell auch im Speziellen, wenn er unvorteilhaft getroffen, halb bekleidet oder nackt ist bzw. intime Handlungen an sich oder anderen vornimmt, wenn also Privat- und Intimsphäre betroffen sind und man sich ehrverletzend über ihn äußern und ihm gegenüber verhalten kann.

13.6 Sicherheit von Cloud-Diensten

Zur Sicherheit und Unsicherheit von Cloud-Diensten existieren viele Einteilungen und Erkenntnisse (vgl. Bedner 2010; Münzl 2015). Im Folgenden werden ein paar wenige Punkte herausgegriffen, die im vorliegenden Kontext besonders relevant sind, und beispielhaft erläutert.

13.6.1 Verschlüsselung und Analyse der Daten

Verschlüsselung sollte auf Benutzerseite vorgenommen werden, also bevor sich die Daten auf den Weg zu den Servern machen. Wo diese stehen und wer Zugang zu ihnen und Zugriff auf sie hat, muss man vor dem Abschluss eines Vertrags abklären. Nicht alle Anwender sind in der Lage, mit kryptografischen Mitteln ihre Daten zu sichern. Sind diese unverschlüsselt auf den Rechnern, kann der Cloud-Anbieter bzw. der Host-Provider im Prinzip semantische Analysen vornehmen (vgl. Kroschwald 2015). Diese mögen dazu dienen, die Kunden und ihre Bedürfnisse besser kennenzulernen, aber ebenso dazu, strafbare Inhalte aufzuspüren. Bekannt wurde, dass Microsoft bei seinen Cloud-Computing-Diensten solche Überprüfungen durchgeführt und Verdächtige

deutschen Ermittlern gemeldet hat (vgl. Mansmann 2015), was man, da es Kinderpornografie betraf, moralisch begrüßen mag, wodurch gleichwohl in die Privatheit eingegriffen wurde, was ethisch zu hinterfragen ist. Zudem weiß der Benutzer nicht, wie die Algorithmen funktionieren. Selbst bei verschlüsselten Daten sind gewisse Analysen möglich, etwa in Bezug auf die Art und Häufigkeit des Zugriffs.

13.6.2 Löschung von Daten

Eine Löschung der Daten kann durch den Cloud-Anbieter bzw. den Host-Provider oder durch einen Angreifer erfolgen. Erstere bereinigen den Bestand aufgrund menschlichen Versagens oder technischer Fehler. Sie können auch der Meinung sein, dass Daten nicht den Nutzungsbestimmungen entsprechen, etwa Fotos oder Texte pornografisch oder rassistisch seien. Zweiterer will bestimmte oder alle Dateien eliminieren, um Spuren zu verwischen oder Schaden beim anderen anzurichten bzw. Nutzen für sich selbst zu stiften. Manche Daten müssen aus gesetzlichen Gründen in bestimmten Zeitabständen gelöscht werden, wobei in diesem Kontext und mit Blick auf den Privatuser vor allem Metadaten betroffen sind. Ein Spezialfall ist die versehentliche oder absichtliche (aber nicht durchdachte) Löschung durch den Benutzer. In vielen Fällen (und in den meisten bei klassischen Speicherdiensten) können die vernichteten Daten wiederhergestellt werden, was allerdings zusätzliche Probleme aufwirft und nach Lösungen verlangt, bis hin zum Recht auf Vergessenwerden (vgl. Mayer-Schönberger 2010). Eine dauerhafte Löschung, die der Benutzer nicht wünscht, kann ihm erhebliche private und berufliche Nachteile bescheren, z. B. weil er einen Vorgang, eine Begebenheit, eine Anstellung oder einen Abschluss nicht mehr nachweisen kann, und seine digitale Identität beschädigen.

13.6.3 Wegfall oder Ersetzung des Anbieters

Der Anbieter kann insolvent werden oder aus rechtlichen bzw. politischen Gründen gezwungen sein, seine Dienste einzustellen, etwa weil das Land unsicher geworden oder aus einem Verbund wie der EU ausgetreten ist. Bei Geschäftsaufgabe werden Rechenzentren u. U. an andere Anbieter verkauft, die neue Regelungen einführen. Der Benutzer ist womöglich weder mit dem geänderten Standort noch mit den geänderten Bestimmungen einverstanden, und es ist denkbar, dass er schlechter gestellt ist, sowohl finanziell als auch informationell, bzw. Zustände und Prozeduren erleiden muss, die nachteilig für ihn sind. Die Daten können ferner an Subunternehmer ausgelagert werden; der Cloud-Anbieter ist nicht durchgehend der Host-Provider (vgl. Kroschwald 2015). Dadurch verbreiten sie sich weiter, ohne dass der Benutzer immer weiß, wo sie liegen und wer darauf zugreifen kann; im Extremfall weiß dies nicht einmal der Anbieter. Im schlimmsten (und seltensten) Fall werden bei Insolvenz die Rechenzentren aufgelöst, und der Benutzer ist nicht mehr in der Lage, an seine Daten heranzukommen. Dies mag ihm wiederum erhebliche Nachteile bescheren und seine digitale Identität beeinträchtigen.

13.6.4 Einsichtnahme in die Datensammlungen

Eine Einsichtnahme in die Datensammlungen kann in manchen Staaten legal erfolgen, in den USA etwa auf der Grundlage des Patriot Act. Durch diesen sind u. a. „der Zugriff auf Kundendaten zum Zwecke der Strafverfolgung“ und „die geheimdienstliche Untersuchung zur Terrorismusbekämpfung“ (Kroschwald 2015) möglich. Der europäische Benutzer, der Cloud-Dienste in Anspruch nimmt, die in den Vereinigten Staaten angesiedelt sind, muss damit nicht nur nationales und europäisches, sondern auch US-amerikanisches Recht beachten; natürlich bezieht sich das genauso auf andere Standorte, und die Unmöglichkeit dieser Aufgabe liegt auf der Hand. Einerseits kann die informationelle Selbstbestimmung verletzt und die Privatsphäre beeinträchtigt werden, andererseits muss der Benutzer strafrechtliche Konsequenzen und Einschränkungen seiner Reisefreiheit fürchten.

13.6.5 Beschlagnahmung oder Diebstahl der Server

Bei Beschlagnahmung oder Diebstahl der Server geraten die Daten in andere bzw. falsche Hände. Ist keine Verschlüsselung erfolgt, können Behörden oder Banden unmittelbar auf die Daten zugreifen. Gibt es keine weiteren Sicherungen, droht neben einem Missbrauch der Daten auch Datenverlust. Dies kann dem Benutzer wiederum Nachteile bescheren und seine digitale Identität beeinflussen. Dabei ist besonders störend, dass offizielle oder kriminelle Kräfte am Werk sind, denen man ausgeliefert ist. Die informationelle Selbstbestimmung ist damit in erheblichem Maße bedroht, und der Schaden kann dauerhaft angerichtet und weltweit erkennbar sein. In Ausnahmefällen sind auch Vorteile möglich, etwa wenn fremderstellte, problembehaftete digitale Identitäten verloren gehen.

13.6.6 Erpressungsversuche

Bestechungs- und Erpressungsversuche können sich auf die Mitarbeitenden der Unternehmen beziehen. Externe können interessiert sein an Fotografien von Prominenten und Betuchten sowie an Inhalten anderer Personen, um wiederum Erpressungsversuche zu starten. Auch die Mitarbeitenden selbst mögen Benutzer unrechtmäßig ausbeuten. Durch Erpressung, in Verbindung mit entsprechendem Datenklau (oder unerwünschten Datengeschenken), werden Privatsphäre bzw. informationelle Autonomie in Frage gestellt und Persönlichkeitsrechte der Benutzer verletzt. Neben den Inhalten selbst können Metadaten weitergereicht werden, wodurch für den Benutzer potenziell zusätzlicher rechtlicher und moralischer Schaden entsteht. So ist es u. U. für Strafverfolgungsbehörden und Gerichte bzw. für die Gesellschaft ein Unterschied für die Bewertung, ob strafbare oder unmoralische Inhalte einmalig oder häufig hochgeladen und aufgerufen werden.

13.7 Konsequenzen für den Benutzer

Gelangen Daten des Benutzers in die Hände von Unbefugten, können sich daraus, wie verschiedentlich angedeutet, erhebliche Konsequenzen ergeben. Im Folgenden werden im Kontext des Cloud Computing strafrechtliche Verfolgung bzw. strafrechtlicher Vollzug, gesellschaftliche Ächtung, Mobbing und Denunziation im persönlichen Umfeld sowie Beeinträchtigung der digitalen Identität näher betrachtet.

13.7.1 Strafrechtliche Verfolgung und strafrechtlicher Vollzug

Eine mögliche Konsequenz ist die strafrechtliche Verfolgung. Diese kann stattfinden, nachdem der Cloud-Anbieter bzw. Host-Provider oder ein Benutzer eine Behörde informiert oder die Polizei selbst bestimmte Inhalte entdeckt hat (vgl. Mansmann 2015). Der Verdacht, unerlaubtes Material (etwa Kinderpornografie) zu besitzen, kann sich erhärten oder eben nicht. Bei Reisen kann es passieren, dass die örtlichen und nationalen Behörden aktiv werden und man nach dortigem Recht festgehalten und verurteilt wird. Dies ist zum einen angängig, wenn die Inhalte des Anwenders auf dem Server gegen die Bestimmungen des entsprechenden Landes verstoßen (wie Karikaturen von Propheten oder Göttern). Zum anderen kann über die Synchronisierung ein Gerät, das vor dem Grenzübertritt sozusagen aufgeräumt wurde, mit strafbaren Inhalten aus der Cloud wiederbeladen werden. Dies ist natürlich eine grundsätzliche Gefahr. Während lokal gespeicherte Inhalte mit Hilfe bestimmter Methoden gelöscht werden können, ist eine dauerhafte Entfernung auf fremden Servern für den Benutzer u. U. schwierig, kaum überprüfbar und nicht unbedingt garantiert. Strafverfolgung und -vollzug haben moralische Implikationen und gefährden das gute Leben des Benutzers. Sind sie für diesen nicht voraussehbar und nicht vereinbar mit dem in seiner Heimat geltenden Recht oder seinem Rechts- und Moralempfinden, stellen sich Fragen der Gerechtigkeit.

13.7.2 Gesellschaftliche Ächtung

Neben Strafverfolgung und -vollzug ist eine gesellschaftliche Ächtung möglich. Dabei muss kein rechtlicher Verstoß des Benutzers vorliegen, sondern es genügt, wenn er aus Sicht einer Gruppe oder der Bevölkerung moralisch falsch gehandelt hat. Im schlimmsten Falle erfolgt eine Ablehnung durch mehrere Gesellschaften oder durch einen Teil der Weltbevölkerung, mitsamt der üblichen Berichterstattung und Verfolgung in den sozialen Netzwerken (Shitstorms, Cybermobbing und -stalking, Denunziation). Das Foto, das eine junge Amerikanerin auf Facebook hochgeladen hatte und das sie inmitten der Häftlingsbaracken im ehemaligen deutschen Vernichtungslager Auschwitz zeigt, nannten Medien das „schlimmste Selfie aller Zeiten“ (vgl. Krafczyk 2014). Deutlich wird, wie eine private, nicht reflektierte Verhaltens-

weise im Zusammenspiel mit technischer Unterstützung ernste Konsequenzen haben kann. Doch ebenso kann jede reflektierte Verhaltensweise den Zorn nicht reflektierter Zeitgenossen in den sozialen Medien und darüber hinaus erregen.

13.7.3 Ächtung im persönlichen Umfeld

Eine gesellschaftliche Ächtung kann zum Teil von den Betroffenen ertragen werden, wenn Freunde und Bekannte zu ihnen halten. Vielfach geht mit ihr aber eine Ächtung im persönlichen Umfeld einher, werden Beleidigung, Verfolgung, Bedrohung und Überwachung selbst in geschützte Räume sozialer Medien und vertrauter Gebäude gebracht (vgl. Bendel 2016, S. 34). Damit droht die Auflösung von Freundschaften und von Beziehungen (ideelle Werte); außerdem können materielle Werte betroffen sein, wenn finanzielle Abhängigkeiten bestehen. Nicht in allen Fällen werden Geräte, die mit der Cloud verbunden sind, nur von einer Person benutzt. Digitale Kameras verfügen immer häufiger über WiFi- und Cloud-Anschlüsse. So teilen sich Lebenspartner und Familienmitglieder eine Wolke, was in unbeabsichtigte Offenlegungen münden kann.

13.7.4 Digitale Identität

Die Identität des Benutzers ist immer häufiger eine digitale oder eine durch das Digitale wesentlich geprägte. Die Summe des Lebens wird nicht allein gebildet durch Geburt, Kindheit und Jugend, Aus- und Weiterbildungen, Partnerschaften und Erfolge, sondern auch durch das Sammeln digitaler Fotos, das Posten von Blognachrichten, das „Erwerben“ von Likes und Favs etc., womit wiederum Bezug auf das private oder berufliche Leben genommen wird. Wenn die Daten in den lokalen Speichern und auf persönlichen Geräten verloren gehen, sei es durch Diebstahl, Brand- oder Wasserschaden, ist die Sicherung in der Cloud ein Segen. Diese kann die digitale Identität sowohl bilden als auch schützen. Umgekehrt kann in der Wolke genauso Datenverlust entstehen und die digitale Identität von Anbietern und Angreifern manipuliert werden. Wie bereits angedeutet, kann eine fremderstellte digitale Identität auch zum Nachteil von Benutzern gereichen, und es kann von Vorteil sein, wenn sie zerstört wird.

13.8 Empfehlungen für Anbieter

Aus der Unternehmensethik heraus kann mit Verweis auf Konsumentenethik und Verbraucherschutz und unter Einbezug der Informationsethik ein Katalog von Empfehlungen für Anbieter erarbeitet werden. Empfehlungen für die Nutzer sollen an dieser Stelle nicht explizit unterbreitet werden. Implizit sind jedoch einige in den verschiedenen Kapiteln enthalten. Oben wurde bereits bemerkt, dass es wünschenswert wäre, wenn die Betriebe und andere Akteure zur Aufklärung beitragen und den Benutzer vor etwaigen Konsequenzen warnen würden. Überdies ist es sinnvoll,

wenn Verbraucherzentralen ihren Beitrag leisten. Im Folgenden werden Vorschläge genannt, die sich aus der erfolgten Behandlung der Risiken ableiten lassen und rechtliche oder ethische Implikationen aufweisen:

- Informierung der Benutzer in Bezug auf die Risiken der Cloud-Dienste, in transparenter Art und Weise und in knapper und verständlicher Form (womöglich unter Verwendung sogenannter Leichter oder Einfacher Sprache), um Informationsgerechtigkeit und -freiheit zu schaffen; von Microsoft wurde etwa eine parallele Führung von Kurz- und Langtexten umgesetzt
- Erhöhung der technischen und organisatorischen Sicherheitsstandards, insbesondere bei der Löschung von Daten, bei Hacking- und Diebstahlversuchen, um u. a. informationelle Autonomie zu bewahren
- Minimierung von Risiken durch sorgfältige Auswahl von Partner- und Subunternehmen, etwa in Bezug auf das Hosting, um u. a. informationelle Selbstbestimmung zu schützen; insbesondere sind auch die Serverstandorte immer wieder einer Prüfung zu unterziehen
- Weiterbildung der Mitarbeitenden, auch auf der Managementebene, in Bezug auf ethische Begriffe und Konzepte (informationelle Autonomie, digitaler Graben etc.) und auf Corporate Social Responsibility
- Weiterbildung der Mitarbeitenden in Bezug auf rechtliche Regelungen (Recht auf informationelle Selbstbestimmung, Urheberrecht, Verwertungsrecht, Persönlichkeitsrecht), wiederum mit Blick auf Corporate Social Responsibility
- Verbesserung des Compliance-Managements und Etablierung von Compliance-Management-Systemen, wobei rechtlichen und ethischen Anforderungen und der zunehmenden Sensibilisierung des Verbrauchers genügt werden muss (vgl. Münzl 2015, S. 41 f.)
- Engagement im gesellschaftlichen, politischen und verwaltungstechnischen Diskurs, um Volksabstimmungen und Gesetzesänderungen zu erreichen und um Behördenzugriffe zu minimieren; Initiierung von entsprechenden Onlinepetitionen

Damit sind nur wenige und allgemeine Punkte genannt. Die Branchen und Betriebe müssen Chancen und Risiken selbst bewerten und zu spezifischen Anforderungen gelangen (vgl. Münzl 2015). Sie werden ein Interesse haben, ein Bündel von Maßnahmen umzusetzen, um bestehende Kunden zu halten und neue zu gewinnen, also aus wirtschaftlichen Gründen, und um moralische und rechtliche Aspekte zu berücksichtigen, was sowohl mit einer intrinsischen Motivation als auch mit einer extrinsischen Prävention (mithin der Abwehr von Ansprüchen und Verfolgungen) verknüpft sein kann.

13.9 Cloud-Anbieter in der Pflicht

Cloud-Computing-Dienste, als spezielle Lösungen oder in Form von sozialen Medien, sind praktisch und verbreitet. Sie helfen dem Endbenutzer dabei, Daten zu sichern, zu bewahren und seine digitale Identität zu wahren. Zugleich liefert er seine

Daten einem oder mehreren Unternehmen und u. U. Behörden und Hackern aus; letztlich transferiert er seine privaten Daten auf fremde Rechner. Natürlich ist das Vorhalten in lokalen Speichern ebenfalls ein Risiko, wenn man an Einbrüche und die erwähnten Wasser- und Brandschäden denkt. Dennoch kann man i. d. R. besser einschätzen, ob jemand auf die Daten zugegriffen hat und ob diese konsistent sind oder korrumpiert wurden.

Aus Sicht von Informationsethik und Verbraucherschutz stellen sich etliche Fragen, und es liegt im Interesse der Cloud-Anbieter, diese befriedigend zu beantworten. Wie deutlich wurde, können sie ganz konkrete Schritte veranlassen. Dabei mögen sie auch die Unterstützung von Verbraucherzentralen und von Wirtschaftsethikern einfordern, wobei sich diese mit Informationsethikern verständigen müssen (vgl. Bendel 2013). Dafür wiederum sind die Hochschulen entsprechend auszustatten, und schon auf Primar- und Sekundarstufe muss, etwa in der Philosophie und speziell in der Ethik, ein Interesse für existenzielle, moralische und soziale Fragen geweckt werden.

Literatur

Abts D, Mülder W (2013) Grundkurs Wirtschaftsinformatik – Eine kompakte und praxisorientierte Einführung, 8. Aufl. Springer, Wiesbaden

Atchison A, Mickeleit T, Rossi C (Hrsg) (2014) Social Business: Von Communities und Collaboration. Frankfurter Allgemeine Buch, Frankfurt am Main

Bedner M (2010) Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung. Kassel University Press, Kassel

Bendel O (2012a) Verbraucherzentrale. Gabler Wirtschaftslexikon. Springer Gabler, Wiesbaden. http://wirtschaftslexikon.gabler.de/Definition/verbraucherzentrale.html. Zugegriffen am 28.04.2016

Bendel O (2012b) Informationsethik. Gabler Wirtschaftslexikon. Springer Gabler, Wiesbaden. http://wirtschaftslexikon.gabler.de/Definition/informationsethik.html. Zugegriffen am 28.04.2016

Bendel O (2013) Die Medizinethik in der Informationsgesellschaft: Überlegungen zur Stellung der Informationsethik. Informatik-Spektrum 36(6):530–535

Bendel O (2016) 300 Keywords Informationsethik: Grundwissen aus Computer-, Netz- und Neue-Medien-Ethik sowie Maschinenethik. Springer Gabler, Wiesbaden

Köhler TR (2012) Die Internetfalle: Google+, Facebook, Staatstrojaner – Was Sie für den sicheren Umgang mit dem Netz wissen müssen. Frankfurter Allgemeine Buch, Frankfurt am Main

Krafczyk E (2014) Die unappetitlichen Selfies von Auschwitz. DIE WELT, 29 Aug 2014. http://www.welt.de/geschichte/zweiter-weltkrieg/article131710140/Die-unappetitlichen-Selfies-von-Auschwitz.html. Zugegriffen am 04.07.2016

Kroschwald S (2015) Informationelle Selbstbestimmung in der Cloud: Datenschutzrechtliche Bewertung und Gestaltung des Cloud Computing aus dem Blickwinkel des Mittelstands. DuD-Fachbeiträge. Springer, Wiesbaden

Kuhlen R (2004) Informationsethik: Umgang mit Wissen und Informationen in elektronischen Räumen. UVK, Konstanz

Mansmann U (2015) Microsoft meldet Kinderpornografie in Cloud-Diensten an deutsche Ermittler. heise online, 12 Jan 2015. http://www.heise.de/newsticker/meldung/Microsoft-meldet-Kinderpornografie-in-Cloud-Diensten-an-deutsche-Ermittler-2516510.html. Zugegriffen am 04.07.2016

Mayer-Schönberger V (2010) Delete: Die Tugend des Vergessens in digitalen Zeiten. Berlin University Press, Berlin
Münzl G (2015) Cloud Computing als neue Herausforderung für Management und IT. Springer, Wiesbaden
Noll B (2013) Wirtschafts- und Unternehmensethik in der Marktwirtschaft. Kohlhammer, Stuttgart
Repschläger J, Pannicke D, Zarnekow R (2010) Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale. HMD Prax Wirtschaftsinformatik 47:6–15
Rohrlich M (2013) Wie sieht das Urheberrecht in der Wolke aus? PC Magazin, 19 Juni 2013. http://www.pc-magazin.de/ratgeber/cloud-online-recht-urheberrecht-ratgeber-1500629.html. Zugegriffen am 04.07.2016