APuZ
Aus Politik und Zeitgeschichte
5–6/2006 · 30. Januar 2006

Digitalisierung und Datenschutz

Beilage zur Wochenzeitung Das **Parlament**

Editorial

Mitte der achtziger Jahre sorgte die bevorstehende Volkszählung in der alten Bundesrepublik für Aufruhr. Eine starke Protestbewegung rief zum Boykott auf. Per Fragebogen wurden schließlich 1987 Haushaltsgrößen, Wohnverhältnisse, Altersstruktur und Arbeitsstätten ermittelt. Der „Zähler“ ging damals von Haus zu Haus.

Mit der Digitalisierung der Kommunikation im 21. Jahrhundert wurden ganz neue Voraussetzungen für eine vernetzte Datensammlung geschaffen. Bei der Zahlung mit Kredit- und Kundenkarten, bei Online-Buchungen, beim Surfen im Internet, bei der Nutzung von Mobiltelefonen und bei der Mauterfassung entstehen Datenspuren, die „verdachtsunabhängig“ gespeichert werden. Zudem schreitet die elektronische Überwachung öffentlicher Räume fort. Immer kleinere, „intelligente“ Funketiketten sowie biometrische Kennzeichen in Personaldokumenten sind Vorboten einer neuen, vernetzten Welt, in der umfassende Datenspeicher miteinander kommunizieren. Mit der Sammelwut wächst auch der Datenmüll. Stehen beispielsweise die Erträge des globalen Lauschangriffs via Satellit und Internet im Verhältnis zum Aufwand? Von den Terroranschlägen des 11. September 2001 wurden die Geheimdienste der USA offenbar völlig überrascht. Doch angesichts terroristischer Bedrohungsszenarien ist die Bereitschaft groß, im Namen der Sicherheit das Private sorglos preiszugeben.

Nicht nur das demokratische Freiheitsrecht auf informationelle Selbstbestimmung, sondern auch das kulturelle Gedächtnis steht im digitalen Zeitalter zur Disposition. Super-8-Filme, Dias, Videobänder, Disketten und selbst CD-ROMs sind Medien der Vergangenheit. Auf ihnen gespeicherte Daten drohen in naher Zukunft unwiederbringlich verloren zu gehen.

Hans-Georg Golz

Manfred Osten

Digitalisierung und kulturelles Gedächtnis

Essay

Ein russisches Sprichwort besagt: „Wer die Vergangenheit anfasst, verliert ein Auge. Wer aber die Vergangenheit vergisst, verliert beide Augen.“ Haben wir beide Augen verloren? Wenn ja, wo liegen die Ursachen dafür? Gibt es eine Geschichte des erodierenden Gedächtnisses, die erklärt, warum wir heute, wie es der Ägyptologe und Gedächtnisforscher Jan Assmann formuliert hat, eine „Gesellschaft des Vergessens“ sind?[1]

Manfred Osten
Dr. jur., geb. 1938; Generalsekretär a. D. der Alexander von Humboldt-Stiftung. Jean-Paul-Straße 12, 53173 Bonn.

Man könnte gegen diese Vermutung einwenden, dass zum Beispiel seit weit mehr als einem Jahrzehnt in Deutschland nicht mehr von einem Vergessen der Geschichte des Nationalsozialismus die Rede sein kann. Allerdings hat Karl Heinz Bohrer mit guten Gründen darauf hingewiesen, dass unsere Erinnerungskultur sich in Wahrheit nur als ein historisches „Nahverhältnis“ manifestiere. Es fehle jedes „Fernverhältnis“ zur Geschichte: „Die Nichtexistenz eines Verhältnisses zur geschichtlichen Ferne, das heißt, zur deutschen Geschichte jenseits des Bezugsereignisses Nationalsozialismus, das wird sofort evident, ist nicht das Resultat eines Willensaktes, der heute oder morgen revidierbar wäre, sondern ist eine Art mentales Apriori, eine zweite Haut bundesrepublikanischen Bewusstseins.“[2] Bohrer hat diese „zweite Haut“ definiert als „vollkommenen Verlust jeder Erinnerung an eine national-orientierte kollektive Vergangenheit“. Diese Erinnerungslosigkeit werde allerdings „verdeckt durch die memoria-Rede, die zu einem Kitsch-Ritual der akademischen Intelligenz zu pervertieren drohe“.

Nach Einschätzung Peter Kümmels spricht gegen diesen Befund bundesdeutscher Erinnerungslosigkeit auch keineswegs die Tatsache neuerer und neuester erinnerungsorientierter Fernsehsendungen. Es handele sich hierbei vielmehr um erinnerungsschonende Pauschalreisen in die NS-Vergangenheit, die das Verdikt Sigmund Freuds einlösen, nach dem man sich erinnere, um zu vergessen. Da aber eine solche Strategie des Vergessens „für die Deutschen nicht statthaft ist, wählen sie gern eine Art der Erinnerung, die dem Vergessen nahe kommt. Es ist die Erinnerung als Zerstreuung.“[3]

Nun könnte man hilfesuchend einwenden, dass ja gerade die Bundesrepublik eine inflationsartige Fülle von historischen Ausstellungen – von den Staufer- und Preußen-Ausstellungen bis hin zur umstrittenen Schau „Verbrechen der Wehrmacht“ – vorweisen könne. Aber auch hier fehlt, nach Bohrers Einschätzung, jedes historische Langzeitgedächtnis. Es handele sich vielmehr nur um scheinbar Kontinuität behauptende Events und Happenings des Erinnerns: „Das seit den 80er Jahren aufgetauchte Interesse breiter Bevölkerungsschichten an früheren Kulturen (. . .) kann nicht für die hier veranschlagte Fernerinnerung in Anspruch genommen werden. Bei solchen Geschichtsinszenierungen, die heute einer generellen Ausstellungspraxis der großen Museen entsprechen, wird eine neue Art des durchaus legitimen Voyeurismus angesprochen, in dem sich eine von Abstraktionen übermüdete Gesellschaft ausruht: Bilder statt Buchstaben, beziehungsweise Argumenten. Mit historischer Fernerinnerung (. . .) hat das wenig zu tun. Eher zeigt sich hier das eigentümliche Phänomen einer unendlichen

[1] Vgl. allgemein zum Thema dieses Essays: Symposium „Das kulturelle Gedächtnis im 21. Jahrhundert“ am 23. 4. 2005 in Karlsruhe, dort der Vortrag von Manfred Osten, Gespeichert, das heißt vergessen – moderne Speichertechnologien, Aufbewahrungspraktiken und gesellschaftliche Implikationen, http://digbib.ubka.uni-karlsruhe.de/diva/2005–314; ferner Manfred Osten, Das geraubte Gedächtnis. Digitale Systeme und die Zerstörung der Erinnerungskultur, Frankfurt/M. 2004.

[2] Karl Heinz Bohrer, Ekstasen der Zeit, München 2003, S. 20 f.; dort auch die folgenden Zitate.

[3] Peter Kümmel, Ein Volk in der Zeitmaschine, in: Die Zeit, Nr. 10 vom 26. 2. 2004, S. 41.

Gegenwart, die sowohl Vergangenheit als auch Zukunft auf das ewige Jetzt kulturellen Konsums schrumpfen lässt."[4] In der fehlenden Fernerinnerung sieht Bohrer den wesentlichen Grund für die Unfähigkeit der Nachkriegsdeutschen zu trauern und für die Schwierigkeiten, das Holocaust-Mahnmal in Berlin zu akzeptieren: „Denn selbst ein Gedächtnis, das sich des Holocaust bewusst ist, (. . .) verdient nur dann diesen Namen, wenn es sich nicht nur der Holocaust-Zeit, sondern der Zeit und der Zeiten bewusst ist, die vor dieser Zeit liegen."[5]

Wie aber müsste sich ein solches Bewusstsein konstituieren? Es müsste vor allem der Einsicht Kierkegaards in den grundsätzlichen Ambivalenz-Charakter des Gedächtnisses geschuldet sein: Dass nämlich das Leben zwar vorwärts gelebt, aber nur rückwärts verstanden wird. Beide Richtungen der Zeitachse, die Zukunft wie die Herkunft, müssten im Interesse einer erfolgreichen Bewältigung der Gegenwart im Blick behalten werden. Das heißt einerseits, Nietzsches Gedanken beherzigen: „Wer handeln will, muss vergessen können." Aber es heißt auch andererseits, zu beherzigen, dass, wer die Vergangenheit vergisst, dazu verdammt ist, sie zu wiederholen. Hinzu kommt, dass ein Minimum an Gedächtniskultur konstitutiv ist für die Entwicklung von Urteilskraft, Qualitätsbewusstsein und Humanität – mit der Konsequenz, dass das Ziel jeder Erziehung die Entwicklung gedächtnisgestützter Urteilskraft sein müsste. Bildung mit dem Ziel bloßer Vermittlung von Zukunftskompetenz ohne Herkunftsgedächtnis erscheint demnach als problematische Zukunftsvorsorge. Denn eine Ausbildung, die vorrangig auf die Vorbereitung für einen zur Zeit marktgängigen Beruf ausgerichtet ist, läuft Gefahr, auf künftige neue Berufsfelder nicht ausreichend reagieren zu können. Nur eine gedächtnisgestützte Urteilskraft wird über jenen Bildungsmehrwert verfügen, der sich nicht allein an einer zur Ideologie geronnenen Betriebswirtschaftslehre mit rein monetärer Kosten-Nutzen-Rechnung orientiert.

Die volkswirtschaftlichen Folgen des grassierenden Mangels einer gedächtnisgestützten Kultur zeigen sich beispielsweise im zuletzt (August 2005) veröffentlichten Arbeitsmarkthandbuch des Nürnberger Instituts für Arbeitsmarkt- und Berufsforschung (IAB): Von rund 2,8 Millionen Arbeitslosen, die seit mehr als einem Jahr ohne Beschäftigung sind, besitzt ein wesentlicher Teil keine Berufsausbildung oder verfügt nur über veraltete Fachkenntnisse. Zurzeit werden rund 400 000 Jugendliche durch berufsvorbereitende Maßnahmen der Bundesagentur für Arbeit (BA) „nachqualifiziert" – in einem Bildungs-Reparaturbereich, für den jährlich 1,2 Milliarden Euro aufgewendet werden müssen und der bereits ein Fünftel jedes Jahrganges betrifft. Die IAB-Chefin Jutta Allmendinger kommentiert: Diese Jugendlichen seien „nicht dumm geboren", sondern würden durch das deutsche Bildungssystem „dumm gemacht (. . .). Wir vergeuden die wichtigste Zukunftsressource in erheblichem Umfang."[6]

Gedächtnisgestützte Herkunftskompetenz muss indes in die Irre führen, wenn sie sich als Selbstzweck einer bloßen Restauration des Vergangenen versteht. Erinnert sei an das Amnesiegebot im antiken Griechenland. Amnesie, das Nicht-Erinnern, hatte sich schon früh als probates Mittel einer Friedensstrategie erwiesen. Um Bürgerkriege und endlose Revanchekriege zu vermeiden, wurde daher das kollektive Vergessen vergangener Fehler und Gräueltaten verordnet, eine Art „Flurbereinigung des Gedächtnisses" zur Sicherung von Gegenwart und Zukunft. In diesem Sinne hat Cicero drei Tage nach Cäsars Ermordung ein Amnesiegebot verkündet. Sogar die Schlussakte des Friedensschlusses von Osnabrück und Münster zur Beendigung des Dreißigjährigen Krieges enthält eine Amnesie. Und noch Ludwig XVIII. hat Amnesie verkündet im Hinblick auf die Schandtaten der französischen Revolutionäre gegenüber seinen Vorfahren.

Das Erodieren des kulturellen Gedächtnisses

Andererseits ist mit der Französischen Revolution auch jenes Phänomen verschwistert, das eingangs angedeutet wurde: jene Geschichte eines raschen Erodierens des kulturellen Gedächtnisses, dessen Spätfolgen

[4] K. H. Bohrer (Anm. 2), S. 14.
[5] Ebd., S. 51.
[6] Zit. in: Frankfurter Allgemeine Zeitung vom 19. 8. 2005, S. 11.

sich bis in die Gegenwart verfolgen lassen. Die Französische Revolution hatte 1792 radikal mit dem alten Gedächtnis, mit 1800 Jahren christlicher Tradition Europas, gebrochen. Denn 1792 endete (mit der Ausrufung des Jahres 1 des Revolutionskalenders) die bisherige christliche Zeitrechnung nach dem Gregorianischen Kalender. Und es blieb Napoleon 1803 vorbehalten, im Wege des Reichsdeputationshauptschlusses in Regensburg den Traditionsbruch, das Zerreißen der Ankerketten der alten Zeit, zu vollenden durch die Auslöschung des Gedächtnisses der Kirchen, Klöster, Archive und Bibliotheken.

Goethe hat früh am Beispiel dieses Vergangenheitshasses der Französischen Revolution und der nachfolgenden Säkularisation bemerkt, dass sich das kulturelle Gedächtnis im Umbau befindet und wir nur deshalb keine Barbaren sind, weil „noch Reste des Altertums“ um uns sind. Er versuchte im „West-Östlichen Divan“, dem rapiden Erodieren des kulturellen Gedächtnisses zu begegnen: „Wer nicht von dreitausend Jahren / sich weiß Rechenschaft zu geben, / mag im Dunkeln unerfahren / von Tag zu Tage leben.“ Die Folgen dieses sich rasch verkürzenden Gedächtnisses brachte er lakonisch auf die Formel: „Nichts Entsetzlicheres als tätige Unwissenheit“. Und es war Franz Grillparzer, der schon 1848 das „Entsetzliche“ dieser „tätigen Unwissenheit“ mit einer Formulierung über den Gang der „neueren Bildung“ zugespitzt hat: „Von der Humanität über die Nationalität zur Bestialität“.

Goethe hatte die Folgen einer gedächtnislosen Fortschritts-Idolatrie im II. Teil der „Faust“-Tragödie vorweggenommen: Faust, der bereits im Hinblick auf die Schleifspur seiner Untaten im Tau von Lethes Fluten Orgien des Vergessens feiert, agiert im 5. Akt als Protagonist eines modernen Vergangenheitshasses. Er lässt die „Überreste des Altertums“ beseitigen, die Goethe als letztes Bollwerk gegen eine gedächtnislose Barbarei verstanden hatte. Er lässt Philemon und Baucis auslöschen mit der Konsequenz, dass damit auch die mit der alten Gedächtniskultur verschwisterte Metaphysik eliminiert wird: Der unerkannt unter den Menschen wandelnde Göttervater Zeus, der bei Philemon und Baucis Gastrecht genießt, wird ebenfalls ermordet.

Den II. Teil seines „Faust“ hat Goethe vorsorglich versiegelt. Hierdurch wollte er möglicherweise seinen Zeitgenossen die Einsicht in diese schwarze Büchse der Pandora ersparen. Erst Nietzsche hat Ende des 19. Jahrhunderts diese Büchse wieder geöffnet – mit dem Hinweis, dass der inzwischen erreichte Verlust des kulturellen Gedächtnisses bereits den neuen Menschentyp der „Legionäre des Augenblicks“ hervorgebracht habe. Die barbarischen Traditions- und Gedächtnisbrüche der beiden Weltkriege, die metaphorische Gedächtnisauslöschung der Bücherverbrennung von 1933 und die Liquidation der bürgerlichen Gedächtniskultur in der Folge der 68er Revolte haben die weitere Entwicklung dieses Typs begünstigt. Hinzu kommt das historische Kurzzeitgedächtnis mit dem Jahr 1945 als „Stunde Null“ und der inzwischen zunehmende monetäre Rechtfertigungsdruck für alle gedächtnisgestützten Phänomene und Institutionen vor allem in den Bereichen der Kultur und der Geisteswissenschaften.

Digitale Gedächtnisspeicher

Die damit verbundenen Erosionen des kulturellen, nationalen und individuellen Gedächtnisses werden durch eine Transformation der Speicher des Gedächtnisses begleitet. Die Rede ist von der Verkürzung der Halbwertszeit der digital gespeicherten Memorabilien. Welche Halbwertszeit haben diese Speicher? Wer sind die Archivare? Wie bestimmen die digitalen Betriebssysteme die Art des Erinnerns? In seiner Analyse der „Gegenwartsvergessenheit“ hat Wolfgang Hagen betont, dass Presse, Radio und Fernsehen keine Rücksicht auf die Dauerhaftigkeit einer Speicherung nehmen: „Die Gegenwartsfixierung einer pressemaschinellen und elektronischen Kommunikationstechnologie, die auf der Stipulierung von Individualkonsum gründet, ist gegenüber Vergangenheit indifferent und macht in Bezug auf die Zukunft blind.“[7]

Womit sich die Frage stellt, ob Ähnliches auch für das digital gespeicherte Gedächtnis gilt. Das Verhältnis von vergänglicher und dauerhafter Erinnerungsspur ist inzwischen zu einem globalen Thema avanciert. In das Anfang der neunziger Jahre des vorigen Jahrhunderts ins Leben gerufene UNESCO-Pro-

[7] Wolfgang Hagen, Gegenwartsvergessenheit, Berlin 2003, S. 119.

gramm „Memory of the World“, ein Register für das kollektive Weltgedächtnis, sollen bedeutende Schrift-, Ton-, Bild- und Filmdokumente aufgenommen werden mit dem Ziel, sie digital im Internet zu präsentieren. Das Programm stellt erstmalig eine digitale Langzeitspeicherung des kulturellen Erbes zur Diskussion, und zwar im Hinblick auf Dokumente, die auf der Weltskala als erinnerungswürdig deklariert werden können.

Daraus ergibt sich das Paradoxon, dass ausgerechnet die Memorabilien des kollektiven Langzeitgedächtnisses einem global verfügbaren Speichermedium mit technisch bedingtem Kurzzeitgedächtnis anvertraut werden sollen. Joachim-Felix Leonhard hat diesen Sachverhalt so beschrieben: „Bei kaum einem Bereich, der sich mit Kulturerbe und Bewertungen befasst, ist deshalb die Frage so virulent, wer denn heute – im Zeitalter digitaler Kommunikation und nicht geklärter Langzeitarchivierung zwecks künftiger Verfügbarkeit – entscheidet, an was wir uns morgen erinnern werden. (. . .) Es ist, als ob eine imaginäre Invasion aus der Galaxis stattfände und uns vor die Robinsonfrage stellte. So wie einst Noah befragt wurde, welche Werte und Gegenstände wichtig erscheinen und – in notwendiger Beschränkung bzw. Selektion – in ein kleines Boot, eine Art virtuelle Arche, zu legen seien.“[8] Hans Magnus Enzensberger hat dieses Gespenst so skizziert: „Das rasante Innovationstempo hat nämlich zur Folge, dass die Halbwertszeit der Speichermedien sinkt. Die National Archives in Washington sind nicht mehr in der Lage, elektronische Aufzeichnungen aus den sechziger und siebziger Jahren zu lesen. Die Geräte, die dazu nötig wären, sind längst ausgestorben. Spezialisten, die die Daten auf aktuelle Formate konvertieren könnten, sind rar und teuer, sodass der größte Teil des Materials als verloren gelten muss. Offenbar verfügen die neuen Medien nur über ein technisch begrenztes Kurzzeitgedächtnis. Die kulturellen Implikationen dieser Tatsache sind bisher noch gar nicht erkannt worden.“[9]

Über diese Implikationen streiten sich inzwischen die beiden Fraktionen des digitalen Zeitalters: die Apokalyptiker auf der einen und die Evangelisten auf der anderen Seite. Die digitalen Evangelisten als Anhänger froher Botschaften globaler Natur prophezeien unter anderem das Heraufziehen einer direkten elektronischen Demokratie, den Abbau von Hierarchien und die nachhaltige Nutzung von Ressourcen. Die digitalen Apokalyptiker verkünden demgegenüber die Schrecken einer Zukunft des „rasenden Stillstands“ im Sinne des Medienphilosophen Paul Virilio und die Gespensterwelt medialer Simulation und Virtualität im Sinne Jean Baudrillards.

Unbestritten ist, dass die digitalen Speichermedien inzwischen eine zentrale Rolle spielen; ihre rasche Entwicklung führt zu Veränderungen, die niemand wirklich abschätzen kann. Sicher ist auch, dass diese Entwicklung das relativ dauerhafte Buchgedächtnis langfristig in einen völlig neuen Aggregatzustand überführen wird. Der Benutzer digitaler Speichermedien, bislang geübt im Umgang mit selbstgenerierten Assoziationen und Einsichten in Verbindungen, findet sich jedenfalls plötzlich wieder als habitualisierter Nutzer von Speicherkapazitäten mit technisch bestimmten formalen Verknüpfungen und der Abhängigkeit von digitalen „Suchmaschinen“. In dem Maße, in welchem sich die Festplatten und Server mit diesen „Digilisaten“ füllen, entleeren sich die Bücherregale der alten Bibliotheken: „Es ist ein verlockendes futuristisches Gedankenspiel: Die Buchbestände der Bibliotheken der Welt, von der nichtigsten Broschüre bis hin zur massiven Enzyklopädie, werden vollautomatisch gescannt. Hochleistungsscanner legen Buch für Buch auf seinen Rücken, scannen Seite für Seite den Buchtext, indem sie das Papier der nachfolgenden Seiten ansaugen und selbstständig umlegen. (. . .) Ein faszinierendes Szenario ist dies, derzeit zwar noch ein wenig utopisch, aber angesichts der rasanten Entwicklungen der IT-Technologie vermutlich in absehbarer Zeit schon als realistisch anzusehen.“[10]

Aber auch diese Hoffnung trügt, zumindest für den Einzelkunden. Denn bereits einfache Rechenexempel zeigen, dass kaum ein

[8] Joachim-Felix Leonhard, Kulturelles Erbe und Gedächtnisbildung, in: Deutsche UNESCO-Kommission (Hrsg.), Lernziel Weltoffenheit. Fünfzig Jahre deutsche Mitarbeit in der UNESCO, Bonn 2001, S. 131.

[9] Hans Magnus Enzensberger, Nomaden im Regal, Frankfurt/M. 2003, S. 122.

[10] Barbara Schneider-Kempf/Martin Hollender, Brauchen wir im digitalen Zeitalter noch Lesesäle? Eine Berliner Antwort, in: Jahrbuch Preußischer Kulturbesitz, 39 (2002), S. 101–114.

künftiger Benutzer über die Finanzkraft verfügen wird, um sämtliche für ihn relevanten Volltexte auf eigene Kosten abzurufen: „Vor allem geistes- und gesellschaftswissenschaftliche Forschungsarbeiten verlangen mitunter nach Dutzenden, ja Hunderten von zu konsultierenden Schriften. Nicht allein Literaturwissenschaftler aber wollen stöbern, sich im Geschriebenen verlieren, zielgerichtet oder ziellos suchen, Anregungen finden, Abseitiges ebenso wie Grundsätzliches entdecken – und zwar in den Bücherregalen des Lesesaales ebenso wie im Kosmos der Netzquellen. Die Chance, Datenmengen zukünftig komfortabel am privaten PC laden zu können, lässt hoffen: Die Notwendigkeit als Einzelkunde, als ‚enduser', horrende Kosten tragen zu müssen, schreckt hingegen ab."[11]

Kollektiver Wissensschwund?

Die zentrale Frage lautet: Muss mit einem kollektiven Wissensschwund auf Grund der raschen Alterungsprozesse der digitalen Systeme gerechnet werden? Nachdem auch das in den letzten 150 Jahren in Büchern mit säurehaltigem Papier materialisierte Gedächtnis Auflösungserscheinungen zeigt, droht den digitalen Gedächtnisträgern eine noch wesentlich kürzere Halbwertszeit des Verfalls. Die Produzenten optischer Gedächtnisspeicher versprechen zwar eine Haltbarkeit von hundert Jahren etwa für CD-ROMs. Aber das Versprechen eines hundertjährigen Langzeitgedächtnisses der optischen Speicherproduzenten ist nicht verifizierbar. Ein Beweis der produktbegleitenden Behauptungen wird nicht angetreten. Und bevor die digitalen Gedächtnisdaten Opfer von Materialermüdung werden, verschwinden bereits jene Geräte, mit denen diese Daten ursprünglich bearbeitet wurden. Hinzu kommt, dass auch die Programme, welche die binären Reihen von Nullen und Einsen in lesbare Information umwandeln können, spätestens auf den Rechnern der übernächsten Generation nicht mehr präsent sind. Inzwischen verlangt die schwindende Dauerhaftigkeit von Hardware zusätzlich neue Strategien des Personalmanagements zur Sicherung digitaler Gedächtnisinhalte. Das bedeutet vor allem die Entwicklung und Aufrechterhaltung spezieller Mitarbeiterfähigkeiten für das Überleben digitaler Informationen angesichts technischer Geräte verschiedener Generationen, Hersteller und Verfahrensweisen.

Die höchste Dringlichkeit dürfte aber angesichts der Unmöglichkeit eines digitalen Langzeitgedächtnisses jene Schlüsseltechnologie beanspruchen, mit der zurzeit die digitalen Evangelisten einen Ausweg aus dem Dilemma ihrer vergänglichen Memorabilien prophezeien: das Storage Area Network (SAN). Das von einer Gruppe („Internet Engineering Task-Force") von Komponenten- und Computerherstellern geplante SAN-System nutzt eine signifikante Eigenschaft digitaler Information: die Unmöglichkeit, Kopien vom Original zu unterscheiden. Eine Langzeit-Überlebensfähigkeit von Memorabilien könnte daher zumindest potenziell durch eine globale Ubiquität digitaler Informationsklone gesichert werden. Das heißt, die jeweilige Information müsste durch digitales „Spiegeln" (*mirroring*) weltweit geografisch verteilt werden – Sicherung also durch wiederholte automatische Spiegelung, eine bereits von der Open-Software-Bewegung implementierte Strategie, die jetzt Teil der SAN-Standards wurde.

Und dies mit doppelter Zielsetzung: Einerseits ermöglicht SAN, dass Datenspeichergeräte mit sehr hoher Speicherkapazität, die an einem bestimmten Ort installiert werden, über private oder auch öffentliche Netzwerke als Komponenten des Computers oder eines lokalen Netzwerks genutzt werden können. Andererseits führt es zur Langzeitsicherung der Informationen regelmäßig Updates durch und überprüft automatisch die Konsistenz aller „gespiegelten", das heißt „verteilten" Kopien. SAN erlaubt die kostengünstige und langfristige Speicherung von Informationen durch die Nutzung von Speichergeräten aller möglichen Hersteller; allerdings unter der Voraussetzung, dass die Produkte dieser Hersteller dem SAN-Standard entsprechen müssen. Das Fazit lautet: „SAN-Spiegelungsstrategien ermöglichen das periodische, vollkommen automatisierte Übertragen von Information von einer Speicherungshardware, die am Ende ihrer Haltbarkeit steht, auf eine neue, die mit dem SAN verbunden ist."[12]

[11] Ebd., S. 106.

[12] Peter Cromwell, Digitale Systeme und Nachhaltigkeit, München 2003, S. 20 f.

Immerhin wären auch bei SAN die Fundamente zunächst weiterhin nicht nur von der Gedächtnisfragilität der Trägermedien geprägt, sondern auch von der Abhängigkeit von Energie und der ständig notwendigen Adaption an aktuelle technische Standards, ganz abgesehen davon, dass auch SAN-Langzeitdaten nicht geschützt sind gegen Naturgewalten. Sicher ist, dass die digitalen Systeme vorteilhaft bleiben werden für diejenigen, die sie mit eigener gedächtnisgestützter Urteilskraft zu nutzen verstehen. Zu den großen Verdiensten der Digitalisierung zählt die damit verbundene Demokratisierung des Wissens im Sinne einer globalen Verfügbarkeit des in Archiven, Bibliotheken und Museen gesammelten kulturellen Erbes.

Die Zukunft des Gedächtnisses

Ein letzter Blick soll der Zukunft der Memorabilien des individuellen und kollektiven Gedächtnisses gelten. Die Rede ist vom CREB (*camp-responsive-element-binding*)-Protein, einer Entdeckung des Neurobiologen Eric R. Kandel, der dafür im Jahr 2000 den Medizin-Nobelpreis erhielt. Das CREB-Protein spielt eine biochemische Schlüsselrolle in jenen neuronalen Aktivitäten des Gehirns, die für die Erinnerung zuständig sind: Es schaltet Gene ein, die für eine stärkere Signalübertragung zwischen zwei Neuronen sorgen, mit dem Ergebnis, dass ein flüchtiger Eindruck dauerhaft im Gedächtnis verankert wird. Sollte es gelingen, dieses Protein künstlich zu produzieren, wären Science-Fiction-Vorstellungen aller Art Tor und Tür geöffnet für die Erinnerungs- und Vergessensgesellschaft der Zukunft.

Inzwischen hat die Neurowissenschaft auch Goethes Erkenntnis bestätigt, dass das Gedächtnis mit dem Interesse wächst. Das heißt, Memorabilien, die emotional positiv begleitet werden, haften offenbar besonders lange im Gedächtnis. Und neurobiologische Forschungsergebnisse der Stanford University haben gezeigt, wie dem Menschen selektives Vergessen gelingt, indem er die Aktivität jener Instanz dämpft, die im Gehirn für den Prozess der Bewusstwerdung und Langzeitspeicherung verantwortlich ist: der Hippocampus. Die gewünschte Verdrängung von Erinnerungen gelingt durch einen gesteigerten Erregungszustand der beiden Seiten des Vorderhirns, des präfrontalen Kortex.

Auch die Geschichtswissenschaft ist inzwischen ins Visier der Hirnforschung geraten: als Epiphänomen neuronaler Vorgänge, die die Vergangenheit immer wieder neu interpretieren und konstituieren, je nachdem, wofür wir im kollektiven Gedächtnis jeweiliger Erinnerungsgemeinschaften sozialen Rückhalt finden. Diese Einsicht hat bereits Walter Benjamin mit seinem Hinweis bestätigt, dass das Gedächtnis nicht etwa ein Instrument zur Erkundung der Vergangenheit sei, sondern vielmehr ihr Schauplatz. Diesem könnten mit Hilfe des CREB-Proteins künftig erhebliche künstliche Eingriffe und Veränderungen drohen in Gestalt von Gedächtnismedikamenten, die bereits in wenigen Jahren zur Auswahl als *memory blocker* oder *memory enhancer* zur Verfügung stehen dürften, mit zurzeit noch unabsehbaren Folgen des Ge- und Missbrauchs.

Das Gedächtnis ist seit den neunziger Jahren des 20. Jahrhunderts auf dem Wege, sich auch zum Leitbegriff einer kulturwissenschaftlichen Neuorientierung zu entwickeln. Und dies als ein transdisziplinärer Forschungsgegenstand, der sich immer mehr gegenüber ganz unterschiedlichen Disziplinen öffnet und seit den neunziger Jahren sogar neue Formen der Vergangenheitspolitik initiiert hat. Verschiedene Staaten haben damit begonnen, sich verstärkt zu einem „negativen Gedächtnis“ zu bekennen, um damit von jenem fragwürdigen heroischen Positiv-Gedächtnis, das bereits Nietzsche als „monumentalische Geschichtsschreibung“ gerügt hat, abzurücken. Für jede Erinnerungsgemeinschaft aber wird weiterhin die unaufhebbare Ambivalenz des Goethe’schen Verdikts gelten: „Wir alle leben vom Vergangenen und gehen am Vergangenen zugrunde.“ Dies könnte auch als Einladung verstanden werden, im Akt des Erinnerns das Heute, die Zukunft und das Vergangene zu umfassen – jenes janusköpfige Bewusstsein also, das zurück und voraus blickt und sich als Aufhebung der Zeit durch Vergessen versteht, und zugleich als Hingabe an die Zeit, der das Gedächtnis Dauer verleiht. Der jüdische Lyriker Paul Celan hat 1952 dieses schwierige Kunststück in ein Gedicht gefasst: „Wir lieben einander wie Mohn und Gedächtnis.“

Alexander Roßnagel

Datenschutz im 21. Jahrhundert

Die Miniaturisierung technischer Komponenten (Prozessoren, Sensoren, Aktoren, Mikrofone und Kameras) schreitet fort. Die Leistung von Rechnern und drahtlosen Kommunikationstechniken wird permanent erhöht, Sensorik und Ortsbestimmung erreichen eine hohe Genauigkeit und die autarke Energieversorgung wird zunehmend leistungsfähiger. Die technischen Komponenten und Dienstleistungen werden zudem immer billiger und breiter verfügbar. Diese technisch-wirtschaftlichen Entwicklungen lassen eine Welt wahrscheinlich werden, in der viele Alltagsgegenstände mit Sensor-, Kommunikations- und Rechnertechnik ausgestattet sind. Die Vision, die Mark Weiser bereits 1990 als *ubiquitous computing* formulierte,[1] scheint Wirklichkeit zu werden. Wir gehen einer Welt entgegen, in der Datenverarbeitung allgegenwärtig geworden ist, aber im Hintergrund abläuft, in der computerisierte Alltagsgegenstände unmerklich und umfassend den Menschen in einer „smarten" Umgebung ihre Dienste anbieten.[2]

Alexander Roßnagel
Dr. jur., geb. 1950; Professor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel und Vizepräsident der Universität Kassel; wiss. Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel; wiss. Direktor des Instituts für Europäisches Medienrecht (EMR) in Saarbrücken. Universität Kassel, Institut für Wirtschaftsrecht, Nora-Platiel-Str. 5, 34109 Kassel.
a.rossnagel@uni-kassel.de

Diese Welt wird neue Chancen für persönliche Entfaltung und Komfort, für Wirtschaft und Arbeit bringen, aber sie stellt auch viele Herausforderungen an die Selbstbestimmung der Individuen. Aus Sicht des Datenschutzes kann der bevorstehende Entwicklungssprung kaum überbewertet werden, denn er stellt die bewährten Regulierungskonzepte in Frage und erfordert die Entwicklung neuer Ansätze des Datenschutzes.

Bereits eine kurze Betrachtung der gemeinsamen Entwicklungsschritte von Informationstechnik und Datenschutz macht dies deutlich.[3] In einer ersten Stufe fand die Datenverarbeitung in Rechenzentren statt. Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens und war – soweit die Daten beim Betroffenen erhoben worden waren – für diesen weitgehend kontrollierbar. Der Betroffene wusste in der Regel, wo welche Daten über ihn verarbeitet wurden. Für diese Stufe der Datenverarbeitung sind die Schutzkonzepte der ursprünglichen Datenschutzgesetze entwickelt worden (dies gilt auch für die europäische Datenschutz-Richtlinie). Die Nutzung von PCs hat die Datenschutzrisiken zwar erhöht, aber nicht auf eine neue qualitative Stufe gehoben.

Die zweite Stufe wurde mit der – weltweiten – Vernetzung der Rechner erreicht. Dadurch entstand ein eigener virtueller Sozialraum, in den nahezu alle Aktivitäten, die in der körperlichen Welt vorgenommen werden, übertragen wurden. Jede Handlung in diesem Cyberspace hinterlässt Datenspuren. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können vom Betroffenen kontrolliert werden. Für die Datenverarbeitung in Deutschland versuchen die Ende der neunziger Jahre erlassenen Multimedia-Datenschutzgesetze, die Risiken in den Griff zu bekommen.[4] Diese Datenverarbeitung betrifft je nach Nutzung des Internets einen großen oder kleinen Ausschnitt des täglichen Lebens,

[1] Vgl. Mark Weiser, The Computer for the 21st Century, in: Scientific American, 265 (1991), S. 94–104.
[2] Vgl. Vlad Coroama u. a., Szenarien des Kollegs „Leben in einer smarten Umgebung – Auswirkungen des Ubiquitous Computing", 2003; Marc Langheinrich/Friedemann Mattern, Digitalisierung des Alltags. Was ist Pervasive Computing?, in: Aus Politik und Zeitgeschichte, (2003) 42, S. 6 ff.; Friedemann Mattern (Hrsg.), Total vernetzt, Berlin 2003; Elgar Fleisch/Friedemann Mattern (Hrsg.), Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Berlin 2005.
[3] Vgl. Alexander Roßnagel, Das rechtliche Konzept der Selbstbestimmung in der mobilen Gesellschaft, in: Jürgen Taeger/Andreas Wiebe (Hrsg.), Mobilität – Telematik – Recht, Köln 2005, S. 54 f.
[4] Vgl. z. B. Alexander Roßnagel, Datenschutz in Tele- und Mediendiensten, in: ders. (Hrsg.), Handbuch Datenschutzrecht, München 2003, S. 1280 ff.

diesen aber potenziell vollständig. Allerdings kann der Betroffene den Risiken des Internets zumindest noch dadurch entgehen, dass er diesen virtuellen Sozialraum meidet.

Mit *ubiquitous computing*, allgegenwärtigem Rechnen, gelangt die Datenverarbeitung in die Alltagsgegenstände der körperlichen Welt – und damit auf eine neue, dritte Stufe. Sie erfasst potenziell alle Lebensbereiche und diese potenziell vollständig. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen verfügbar, Informationen aus der realen Welt in die virtuelle integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es keinen Ausweg.

Insofern verschärft sich das Problem des Datenschutzes radikal, und seine Lösung wird existenziell. Datenschutz wird in einer so skizzierten Welt immer wichtiger, aber er wird auch zunehmend gefährdet sein. Im Folgenden wird das rechtliche Konzept der informationellen Selbstbestimmung für die erste und auch die zweite Stufe beschrieben. Sodann werden die Herausforderungen untersucht, denen dieses Konzept in der dritten Stufe ausgesetzt ist. Schließlich wird versucht, Ansätze zu benennen, die erforderlich sind, um Selbstbestimmung auch in dieser neuen Welt zu ermöglichen.

Informationelle Selbstbestimmung und Datenschutzrecht

Datenschutz ist ein irreführender Begriff, denn es sollen nicht die Daten (des Datenbesitzers) geschützt werden, sondern die informationelle Selbstbestimmung (des Betroffenen). Informationelle Selbstbestimmung lautet für das Bundesverfassungsgericht (BVerfG) die verfassungsrechtliche Antwort auf die besonderen Risiken der automatischen Datenverarbeitung für die Selbstbestimmung des Einzelnen. Dieses Grundrecht hat eine subjektive und eine objektive Schutzrichtung.

Die informationelle Selbstbestimmung schützt zum einen die selbstbestimmte Entwicklung und Entfaltung des Einzelnen. Diese kann nur in einer für ihn kontrollierbaren Selbstdarstellung in unterschiedlichen sozialen Rollen und der Rückspiegelung durch die Kommunikation mit anderen gelingen. Wer dagegen „nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“.[5]

Informationelle Selbstbestimmung ist zugleich die Grundlage einer freien und demokratischen Kommunikationsverfassung. Selbstbestimmung ist „eine elementare Funktionsbedingung eines freiheitlich demokratischen Gemeinwesens“, das „auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger“ angewiesen ist.[6] Informationelle Selbstbestimmung zielt somit auf eine Kommunikationsordnung, die einen selbstbestimmten Informationsaustausch und eine freie demokratische Willensbildung ermöglicht.

Um informationelle Selbstbestimmung wirksam werden zu lassen, verfolgt das Datenschutzrecht das folgende normative Schutzprogramm: 1. Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn der Gesetzgeber oder der Betroffene diese hinsichtlich Umfang und Zweck gebilligt haben. 2. Damit der Betroffene die Datenverarbeitung am Maßstab der gesetzlichen Erlaubnis kontrollieren oder informiert in diese einwilligen kann, muss die Datenverarbeitung ihm gegenüber transparent sein. 3. Die Datenverarbeitung ist nur für den gebilligten Zweck zulässig und darf nur in dem Umfang erfolgen, der erforderlich ist, um diesen zu erreichen. Der Betroffene hat Auskunfts- und Korrekturrechte.

Herausforderungen durch allgegenwärtige Datenverarbeitung

Die Gewährleistung der informationellen Selbstbestimmung durch dieses normative Schutzprogramm ist durch die Entwicklung zu einer allgegenwärtigen Datenverarbeitung gefährdet. Dadurch wird nicht die Notwendigkeit informationeller Selbstbestimmung in Frage gestellt. Wenn die Welt allgegenwärti-

[5] BVerfGE 65, 1 (43) (Volkszählungsurteil).
[6] Ebd.

ger Datenverarbeitung human und lebenswert sein soll, muss diese Selbstbestimmung mehr noch als heute gewährleistet sein. Fraglich ist jedoch, ob das bisherige datenschutzrechtliche Schutzprogramm für dieses Grundrecht noch angemessen ist.[7]

Die meisten Anwendungen allgegenwärtiger Informationstechnik werden von den Betroffenen selbst gewählt und gern genutzt, weil sie ihnen Erweiterungen ihrer geistigen und körperlichen Fähigkeiten bieten, sie bei Routineaufgaben unterstützen, ihnen Entscheidungen abnehmen und das Leben bequemer machen. Sie werden individualisierte Dienste und Geräte fordern, die sich ihnen anpassen, und im Gegenzug – mehr oder weniger notgedrungen – damit einverstanden sein, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweisen, Gewohnheiten, Einstellungen und Präferenzen erhalten. Zwar wird es auch künftig klare und einfache Frontstellungen zwischen Betroffenen und Datenverarbeitern geben, die zum Beispiel Waren mit RFID[8] versehen, diese auswerten und ihren Kunden keine Wahlmöglichkeit lassen. Hierfür werden dem bestehenden Datenschutzprogramm klare Antworten zu entnehmen sein, die den Aufsichtsbehörden ein passendes Verhalten ermöglichen. Im Regelfall werden aber die Verhältnisse komplizierter und schwieriger zu bewerten sein.

Computerisierte Alltagsgegenstände begleiten die Menschen bei ihren Tätigkeiten und unterstützen sie – scheinbar mitdenkend – in einer sich selbst organisierenden Weise. Sie fungieren nicht mehr nur als Träger und Mittler von Daten, sondern generieren Daten selbst, die sie untereinander austauschen, und „entwickeln" ein eigenes „Gedächtnis". Sie werden unmerklich Teil des Verhaltens und Handelns ihrer Nutzer. Sie ermöglichen es, von den Betroffenen sehr präzise Profile über ihre Handlungen, Bewegungen, Beziehungen, Verhaltensweisen, Einstellungen und Präferenzen in der körperlichen Welt zu erzeugen. Interessenten für diese Daten könnten zum Beispiel Anbieter von Waren und Dienstleistungen, Arbeitgeber, Versicherungen, Auskunfteien oder staatliche Überwachungsbehörden, aber auch der neugierige Nachbar oder ein eifersüchtiger Liebhaber sein. Mit der allgegenwärtigen Datenverarbeitung wird eine potenziell perfekte Überwachungsinfrastruktur aufgebaut. Durch die Pflicht von Telekommunikationsanbietern zur Vorratsdatenspeicherung wurde für staatliche Überwachungsbehörden hierzu auch schon ein Zugang eröffnet.

Durch allgegenwärtige Datenverarbeitung werden nicht nur neue Missbrauchsmöglichkeiten eröffnet. Diesen könnte man durchaus mit dem bisherigen Schutzprogramm (und eventuell besser ausgestatteten Aufsichtsbehörden) begegnen. Entscheidender ist, dass durch allgegenwärtige Datenverarbeitung das bisherige Schutzprogramm als solches in jedem seiner Bestandteile in Frage gestellt wird.

So stoßen zum Beispiel die bisherigen Instrumente der *Transparenz* an subjektive Grenzen. Allein die zu erwartende Vervielfachung der Datenverarbeitungsvorgänge in allen Lebensbereichen übersteigt die mögliche Aufmerksamkeit um ein Vielfaches. Zudem soll die allgegenwärtige Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen. Niemand würde es akzeptieren, wenn er täglich tausendfach bei meist alltäglichen Tätigkeiten Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Selbst wenn er dies wollte, stehen oft keine oder keine adäquaten Ausgabemedien zur Verfügung. Außerdem setzen hohe Komplexität und vielfältige Zwecke der möglichen Transparenz objektive Grenzen. Statt eines einfachen Datensatzes (z. B. Postadresse) würde dem Betroffenen bei einer Auskunft über die verarbeiteten Daten ein komplexes Sensordestillat präsentiert, bei dem meist nur vermutet werden kann, dass es die betroffene Person meint.[9] Für viele Anwendungen wird bei der Datenerhebung unklar sein, ob die Daten personenbezogen

[7] Vgl. hierzu auch Alexander Roßnagel/Jürgen Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz. Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze, in: Computer und Recht, (2004), S. 628 ff.

[8] RFID = Radio Frequency Identification. *Anm. der Red.:* Vgl. dazu den Beitrag von Britta Oertel und Michaela Wölk in diesem Heft.

[9] Vgl. auch Marc Langheinrich, Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, www.vs.inf.eth.ch/publ/papers/langhein2004rfid.pdf, S. 12.

sind. Sie erhalten den Personenbezug – wenn überhaupt – oft erst viel später. Vielfach wird die (Mit-)Erhebung von Daten (durch Kamera oder Sensor) sogar unerwünscht sein. Eine Unterrichtung des Betroffenen wird daher vielfach unmöglich oder sehr schwierig sein.

Eine *Einwilligung* für jeden Akt der Datenverarbeitung zu fordern, würde angesichts der Fülle und Vielfalt der Vorgänge und der Unzahl von verantwortlichen Stellen zu einer Überforderung aller Beteiligten führen. Noch weniger umsetzbar wäre es, hierfür die geltenden Formvorschriften – Schriftform oder elektronische Form – zu fordern. Selbst eine Einwilligung in der für das Internet gedachten Form einer elektronischen Bestätigung[10] dürfte unter diesen Umständen meist nicht praktikabel sein. In dieser Welt wird die Einwilligung als Instrument des Datenschutzrechts in bisher bekannter Form nur in generalisierter Anwendung überleben können. Bei vorher bekannten Dienstleistungen werden die Betroffenen in Rahmenverträgen mit allgemeinen Zweckbestimmungen ihre Einwilligung erteilen. Damit wird die Steuerungskraft der Einwilligung für die Zulässigkeit der Datenverarbeitung noch weiter sinken. Für spontane Kommunikationen wird die Einwilligung ihre Bedeutung ganz verlieren.

Die *Zweckbindung* widerspricht der Idee einer unbemerkten, komplexen und spontanen technischen Unterstützung. Je vielfältiger und umfassender die zu erfassenden Alltagshandlungen sind, umso schwieriger wird es, den Zweck einzelner Datenverarbeitungen vorab festzulegen und zu begrenzen.[11] Die klare Bestimmung des Zwecks, der oft durch die funktionale Zuordnung zu einem Gerät abgegrenzt war (zum Beispiel: Fernsprechapparat für Sprachkommunikation), ist nicht mehr möglich. Daher stellt sich die Frage, ob der bereichsspezifisch, klar und präzise festgelegte Zweck, den das BVerfG fordert,[12] noch das angemessene Kriterium sein kann, um die zulässige Datenverarbeitung abzugrenzen.[13] So kann etwa für Ad-hoc-Kommunikation, für die sich die Infrastruktur jeweils situationsabhängig und ständig wechselnd mit Hilfe der Endgeräte der Kommunikationspartner und unbeteiligter Dritter bildet, nicht vorherbestimmt werden, welche Beteiligten zu welchen Zwecken welche Daten erhalten und verarbeiten.[14] Jeder kann ein mobiles Ad-hoc-Netz, sozial betrachtet, für beliebige Zwecke benutzen. Jeder kann in diesem Netz, technisch betrachtet, zeitweise und abwechselnd als Sender, Mittler und Empfänger wirken. Werden dabei die Vorgänge in verschiedenen Lebensbereichen miteinander verknüpft oder werden technische Funktionen miteinander verschmolzen, wechselt der Zweck, zu dem Daten anfänglich erhoben und verarbeitet wurden, mehrfach – ohne dass dies dem vom Gesetzgeber oder dem Betroffenen gewünschten Ziel widerspricht.

Werden aber Daten für vielfältige und wechselnde Zwecke erhoben, sind eine an einem begrenzten Zweck orientierte Abschottung von Daten, ein daran anknüpfender Zugriffsschutz und eine auf der Zweckunterscheidung aufbauende informationelle Gewaltenteilung schwierig zu verwirklichen, vielfach sogar unpassend. Ähnlich verhält es sich mit dem Verbot einer Datenhaltung auf Vorrat und einer Profilbildung. Wenn Anwendungen Erinnerungsfunktionen für künftige Zwecke erfüllen sollen, die noch nicht bestimmt werden können, sind Datenspeicherungen auf Vorrat nicht zu vermeiden. Wenn die Systeme kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, vielfältige Profile erzeugen müssen.

Das Problem der Zweckbindung könnte formal durch eine weite Fassung der Zweckbestimmung gelöst werden. Dadurch wird aber die Steuerungswirkung der Zweckbestimmung nicht verbessert. Im Gegenteil – Generalklauseln wie das „berechtigte Interesse“ und Gebote zur Abwägung mit „schutzwürdigen Interessen“ des Betroffenen[15] wären für die informationelle

[10] Vgl. § 4 Abs. 2 Teledienstedatenschutzgesetz und § 18 Abs. 2 Mediendienstestaatsvertrag.
[11] Vgl. hierzu auch M. Langheinrich (Anm. 9), S. 9.
[12] BVerfGE 65, 1 (44, 46).
[13] Vgl. kritisch aus anderen Gründen Alexander Roßnagel/Andreas Pfitzmann/Hansjürgen Garstka, Modernisierung des Datenschutzrechts, Gutachten für das Bundesministerium des Innern, 2001, S. 29 ff.
[14] Vgl. Stefan Ernst, Rechtliche Probleme mobiler Ad-hoc-Netze, in: J. Taeger/A. Wiebe (Anm. 3), S. 127 ff.
[15] S. §§ 28 und 29 Bundesdatenschutzgesetz.

Selbstbestimmung kontraproduktiv, weil sie praktisch die Datenverarbeitung freigeben und für den Betroffene unkontrollierbar machen.[16] Bleiben solche Generalklauseln bestehen, werden sie bei einer allgegenwärtigen Datenverarbeitung mit neuen Bedeutungen gefüllt. Sie werden in der Praxis die „Freikarte" für alle Interessierten sein, die vielfältigen und umfassenden Datenspuren für ihre Zwecke zu verarbeiten.

Da das Prinzip der *Erforderlichkeit* am Zweck der Datenverarbeitung ausgerichtet ist, erleidet es die gleiche Schwächung wie das Prinzip der Zweckbindung. Soll die Datenverarbeitung im Hintergrund ablaufen, auf Daten zugreifen, die durch andere Anwendungen bereits generiert wurden, und gerade dadurch einen besonderen Mehrwert erzeugen, wird es schwierig sein, für jede einzelne Anwendung eine Begrenzung der zu erhebenden Daten oder deren frühzeitige Löschung durchzusetzen. Auch die Einbeziehung von Umweltbedingungen mittels Sensortechnik in einer dynamischen, laufend aktualisierenden Weise beschränkt zudem die Begrenzungsfunktion des Erforderlichkeitsprinzips. Das Ziel, die Gegenstände mit einem „Gedächtnis" auszustatten, um dadurch das löchrige Gedächtnis des Nutzers zu erweitern, lässt das Erforderlichkeitsprinzip leer laufen.[17]

Aus dem gleichen Grund stößt der Grundsatz der *Datenvermeidung* an Grenzen. Vielfach kann erst eine Vielzahl langfristig gespeicherter Daten die gewünschte Unterstützungsleistung bieten. Auch die Verarbeitung anonymer und pseudonymer Daten kann ungeeignet sein, weil die Daten oftmals unmittelbar erhoben werden: Eine Kamera, ein Mikrofon oder ein Sensor nehmen anders als ein Webformular den Benutzer direkt wahr und können vielfach nicht ohne Offenlegung der Identität des Benutzers verwendet werden. Indirekte Sensoren wie zum Beispiel druckempfindliche Bodenplatten können auch ohne direkte Wahrnehmung primärer biometrischer Attribute durch Data-Mining-Techniken Menschen etwa an ihrem Gang identifizieren. Die für die allgegenwärtige Datenverarbeitung typische enge Verknüpfung der Sensorinformation mit Ereignissen der realen Welt erlaubt selbst bei konsequenter Verwendung von Pseudonymen in vielen Fällen eine einfache Personenidentifikation. So können zum Beispiel bei einem Indoor-Lokalisierungssystem die pseudonymen Benutzer anhand ihres bevorzugten Aufenthaltsortes identifiziert werden.[18]

Mitwirkungs- und Korrekturrechte des Betroffenen werden wegen der Vervielfachung und Komplexität der Datenverarbeitung im Alltag, die oft unmerklich stattfinden wird, an Durchsetzungsfähigkeit verlieren. Außerdem werden die Vielzahl der beteiligten Akteure, die spontane Ver- und Entnetzung sowie der ständige Rollenwechsel zwischen Datenverarbeiter und Betroffenem zu einer Zersplitterung der Verantwortung für die Datenverarbeitung führen. Schließlich werden die verantwortlichen Stellen selbst oft nicht wissen, welche personenbezogenen Daten sie verarbeiten. Vorgänge aber zu protokollieren, um Auskunfts- und Korrekturrechte erfüllen zu können, wäre in vielen Fällen im Hinblick auf Datensparsamkeit kontraproduktiv.

Zusammenfassend ist festzustellen: Alle Bestandteile des überkommenen Schutzprogramms werden durch allgegenwärtige Datenverarbeitung ausgehöhlt oder überspielt. Daher ist die Frage ganz grundsätzlich zu stellen, ob unter diesen Verhältnissen informationelle Selbstbestimmung überhaupt noch möglich ist.

Ansätze zur Wahrung der informationellen Selbstbestimmung

Um informationelle Selbstbestimmung weiterhin zu gewährleisten, muss das normative Schutzprogramm modifiziert und ergänzt werden. In welche Richtung diese Modernisierung des Datenschutzrechts gehen muss, soll kurz angedeutet werden.[19]

Erstens sind die bisherigen Zulassungskontrollen verstärkt durch *Gestaltungs- und Verarbeitungsregeln* zu ergänzen. Statt das Schwergewicht auf eine einmalige, lange vor der Datenverarbeitung liegende Zulassungs-

[16] Vgl. kritisch A. Roßnagel/A. Pfitzmann/H. Garstka (Anm. 13), S. 77 f.
[17] Vgl. auch Friedemann Mattern, Ubiquitous Computing, in: J. Taeger/A. Wiebe (Anm. 3), 28 ff.
[18] Vgl. M. Langheinrich (Anm. 9), S. 11 f.
[19] Vgl. ausführlicher A. Roßnagel (Anm. 3), S. 70 ff.

entscheidung durch Zwecksetzung des Gesetzgebers oder des Betroffenen zu legen, sollte Datenschutz künftig vorrangig durch Gestaltungs- und Verarbeitungsregeln bewirkt werden, die permanent zu beachten sind.[20] So könnte zum Beispiel Transparenz statt auf einzelne Daten stärker auf Strukturinformationen bezogen sein und statt durch eine einmalige Unterrichtung durch eine ständig einsehbare Datenschutzerklärung im Internet gewährleistet werden. Eine andere Transparenzforderung könnte darin liegen, von allen datenverarbeitenden Alltagsgegenständen eine technisch auswertbare Signalisierung zu fordern, wenn sie Daten erheben. Die Einwilligung könnte eine Aufwertung erfahren, wenn sie auf ein technisches Gerät der betroffenen Person „delegiert" werden könnte, das bei jedem signalisierten Verarbeitungsvorgang im Hintergrund die Datenschutz-Policies prüft, akzeptiert oder verwirft.[21] Als ein Einverständnis könnte auch anzusehen sein, wenn der Betroffene bewusst und freiwillig seine individuellen Fähigkeiten unterstützende und verstärkende Techniksysteme und Dienste nutzt. Im Gegenzug müssen diese so gestaltet sein, dass sie über Datenschutzfunktionen verfügen, die er auswählen und für sich konfigurieren kann.[22]

Die Beispiele haben gezeigt, dass diese Gestaltungs- und Verarbeitungsregeln auf technische Umsetzung angewiesen sind. Daher sollte *Datenschutz* zweitens stärker *durch Technikgestaltung* statt durch Verhaltensregeln gewährleistet werden.[23] Informationelle Selbstbestimmung muss durch Infrastrukturen unterstützt werden, die es ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Ein Beispiel: Die Einhaltung von Verarbeitungsregeln zu kontrollieren darf nicht die permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen. Wenn die datenverarbeitenden Alltagsgegenstände ein Signal aussenden, kann dies von einem Endgerät des Betroffenen erkannt werden und zu einer automatisierten Auswertung der zugehörigen Datenschutzerklärung führen. Entsprechend den voreingestellten Datenschutzpräferenzen kann dann ein P3P[24]-ähnlicher Client die Einwilligung erteilen oder ablehnen. In Zweifelsfällen kann das Gerät je nach Voreinstellung den Betroffenen warnen und ihm die Erklärung in der von ihm gewählten Sprache anzeigen oder akustisch ausgeben. Die Hinweis- und Warndichte muss einstellbar sein.[25] Die Durchsetzung von Verarbeitungsregeln muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erreicht werden.[26] Technischer Datenschutz hat gegenüber rein rechtlichem Datenschutz Effektivitätsvorteile: Was technisch verhindert wird, muss nicht mehr verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen nicht. Datenschutztechnik kann so Kontrollen und Strafen überflüssig machen.

Drittens muss *Vorsorge* die Gefahrenabwehr ergänzen, zum einen durch die Reduzierung von Risiken und zum anderen durch präventive Folgenbegrenzungen potenzieller Schäden. Die Risiken für die informationelle Selbstbestimmung sind in einer Welt allgegenwärtiger Datenverarbeitung nicht mehr ausreichend zu bewältigen, wenn nur auf die Verarbeitung personenbezogener Daten abgestellt wird. Vielmehr sind im Sinn vorgreifender Folgenbegrenzung auch Situationen zu regeln, in denen noch gar keine personenbezogenen Daten entstanden sind. So bedürfen zum Beispiel die Sammlungen von Sensorinformationen, Umgebungsdaten oder von pseudonymen Präferenzen einer vorsorgenden Regelung, wenn die Möglichkeit oder gar

[20] Vgl. A. Roßnagel/A. Pfitzmann/H. Garstka (Anm. 13), S. 70 ff.

[21] Vgl. hierzu auch M. Langheinrich (Anm. 9), S. 10 f.

[22] Vgl. auch Alexander Roßnagel, Datenschutz im Jahr 2015 – in einer Welt des Ubiquitous Computing, in: Johann Bizer/Albert von Mutius/Thomas B. Petri/Thilo Weichert (Hrsg.), Innovativer Datenschutz – Wünsche, Wege, Wirklichkeit, Festschrift für Helmut Bäumler, Kiel 2004, S. 335–351.

[23] Vgl. Marit Köhntopp und Burckhardt Nedden, Datenschutz und „Privacy Enhancing Technologies", in: Alexander Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, Baden-Baden 2001, S. 55 ff. und 67 ff.

[24] P3P = Platform for Privacy Preferences, eine internationale, standardisierte Plattform zum Austausch von Datenschutzinformationen im Internet. Der User soll beim Besuch einer Website schnell und automatisiert einen Überblick erhalten, welche Daten der Webanbieter oder Dritte zu welchen Zwecken verarbeiten. Vgl. www.w3c.org/P3P.

[25] Vgl. hierzu auch, allerdings mit skeptischen Hinweisen, M. Langheinrich (Anm. 9), S. 10.

[26] Vgl. z. B. Jürgen Müller/Matthias Handy, RFID und Datenschutzrecht, in: Datenschutz und Datensicherheit, (2004) 11, S. 629.

die Absicht besteht, sie irgendwann einmal mit einem Personenbezug zu versehen.[27] Auch sind zur Risikobegrenzung Anforderungen an eine transparente, datensparsame, kontrollierbare und missbrauchsvermeidende Technikgestaltung zu formulieren. Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme präventiven (freiwilligen) Prüfungen ihrer Datenschutzkonformität zu unterziehen und diese Prüfung zu dokumentieren.

Regelungen, die sich nur an Datenverarbeiter richten, dürften viele Gestaltungsziele nicht erreichen. In viel stärkerem Maß sind daher viertens die *Technikgestalter als Regelungsadressaten* anzusprechen. Diese sollten vor allem Prüfpflichten für eine datenschutzkonforme Gestaltung ihrer Produkte, eine Pflicht zur Dokumentation dieser Prüfungen für bestimmte Systeme und Hinweispflichten für verbleibende Risiken treffen.[28] Auch sollten sie verpflichtet werden, ihre Produkte mit datenschutzkonformen Default-Einstellungen auszuliefern.[29]

Die datenschutzgerechte Gestaltung der künftigen Welt allgegenwärtiger Datenverarbeitung fordert die aktive Mitwirkung der Entwickler, Gestalter und Anwender. Sie werden nur für eine Unterstützung zu gewinnen sein, wenn sie davon einen Vorteil haben. Daher sollte fünftens die Verfolgung legitimen Eigennutzes in einer Form ermöglicht werden, die zugleich auch dem Gemeinwohl dient. Datenschutz muss daher zu einem Werbeargument und *Wettbewerbsvorteil* werden. Dies ist möglich durch die freiwillige Auditierung von Anwendungen, die Zertifizierung von Produkten und die Präsentation von Datenschutzerklärungen. Werden diese von Datenschutzempfehlungen à la „Stiftung Warentest", von Rankings oder durch die Berücksichtigung bei öffentlichen Auftragsvergaben begleitet, kann ein Wettbewerb um den besseren Datenschutz entstehen. Dann werden die Gestaltungsziele beinahe von selbst erreicht.[30]

[27] Vgl. Alexander Roßnagel/Philip Scholz, Datenschutz durch Anonymität und Pseudonymität, in: MultiMedia & Recht, (2000), S. 728 ff.
[28] Vgl. A. Roßnagel/A. Pfitzmann/H. Garstka (Anm. 13), S. 143 ff.
[29] Zur Verantwortung der Informatiker vgl. Alexander Roßnagel, in: Informatik-Spektrum, (2005) 6, S. 462 ff.
[30] Vgl. Alexander Roßnagel, Datenschutzaudit, in: ders. (Anm. 4), S. 439 ff.

Der Schutz der informationellen Selbstbestimmung bedarf schließlich sechstens einer objektiven Ordnung, die in der Praxis mehr und mehr an die Stelle individueller Rechtewahrnehmung tritt. Die Einhaltung von Datenschutzvorgaben kann künftig immer weniger von der individuellen Kontrolle des Betroffenen abhängig gemacht werden. Sie muss in noch viel stärkerem Maß stellvertretend *Kontrollverfahren und Kontrollstellen* übertragen werden, die das Vertrauen der Betroffenen genießen. Gegenstand der Kontrolle müssen Systeme mit ihren Funktionen und Strukturen sein, nicht so sehr die individuellen Daten. Ziel der Kontrolle muss es sein, die individuellen und gesellschaftlichen Wirkungen der technischen Systeme zu überprüfen und diese datenschutzgerecht zu gestalten.

Ausblick

Informationelle Selbstbestimmung wird im 21. Jahrhundert nur gewahrt werden können, wenn ihr Schutzprogramm modifiziert und ergänzt wird. Notwendig ist eine objektivierte Ordnung der Datenverarbeitung und -kommunikation bei professioneller Kontrolle, mit vorsorgender Gestaltung von Strukturen und Systemen, der Inpflichtnahme von Herstellern zur Umsetzung von Datenschutz in Technik sowie der Nutzung von Eigennutz durch Anreize zu datenschutzgerechtem Handeln.

Ob diese neuen Ansätze erfolgreich sind, muss bis zum Beweis durch die Praxis als offen gelten. Sie sind notwendige, keine hinreichenden Bedingungen. Hinzu kommen müssen bei den Individuen das Bewusstsein, dass informationelle Selbstbestimmung ein hohes, aber gefährdetes Gut ist, sowie der Wunsch, es zu bewahren, und in der Gesellschaft die Erkenntnis, dass hierfür Strukturänderungen erforderlich sind, und der politische Wille, sie auch umzusetzen. Ohne die dargestellten Anpassungen dürfte die Vorhersage nicht schwer sein, dass die informationelle Selbstbestimmung schleichend ihrer Bedeutungslosigkeit entgegengeht.

Britta Oertel · Michaela Wölk

Anwendungspotenziale „intelligenter“ Funketiketten

Britta Oertel
M.A., Informationswissenschaftlerin und Geografin; Mitarbeiterin des Instituts für Zukunftsstudien und Technologiebewertung gGmbH (IZT), Schopenhauerstraße 26, 14129 Berlin.
b.oertel@izt.de

Michaela Wölk
M.A., Informationswissenschaftlerin und Volkswirtin; Mitarbeiterin des IZT.
m.woelk@izt.de

Automatisierte Identifikation und Datenerfassung zeichnen sich durch eine schnelllebige Entwicklung aus und sind einer ebenso dynamischen öffentlichen Diskussion ausgesetzt. Die „intelligenten“ Etiketten werden in den Medien auch als Funkchips, Smart Labels oder sogar „Schnüffelchips“ bezeichnet. Diese automatischen Identifikationssysteme heißen in der Fachsprache RFID (Radio-Frequenz- IDentifikation) und sollen traditionelle Lösungen wie den Barcode ersetzen. Die Funktion von RFID besteht darin, Waren, Tiere oder auch Personen über Funk eindeutig und kontaktlos zu identifizieren. Der Einsatz von RFID-Systemen eignet sich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden soll.

Die RFID-Technologie ist eine typische Querschnittstechnologie, die in nahezu allen Lebens- und Wirtschaftsbereichen angewandt werden kann. In ausgewählten Marktsegmenten zeigen RFID-Systeme bereits seit Jahrzehnten eine kontinuierliche Marktentwicklung. In anderen Bereichen werden RFID-Systeme getestet. In der Praxis überwiegen derzeit noch unternehmensinterne Einzellösungen, unter anderem aufgrund unzureichender Standardisierung und zu hoher Investitionskosten. Das Potenzial von RFID-Systemen besteht jedoch insbesondere im unternehmensübergreifenden Einsatz, beispielsweise bei der Warenrückverfolgung über die gesamte Wertschöpfungskette hinweg.

Die Entwicklungsperspektiven der RFID-Technologie hängen nicht allein von den technischen Möglichkeiten ab. Neben Technologie und Standardisierung zählen Wirtschaftlichkeitsberechnungen, Informationssicherheit und Datenschutz sowie die gesellschaftliche Akzeptanz zu den zentralen Erfolgsfaktoren. Gleichzeitig rückt die Frage, ob und in welcher Form zusätzliche datenschutzrechtliche Regelungen durch den breiteren Einsatz von RFID-Systemen erforderlich sind, verstärkt in den Mittelpunkt der gesellschaftlichen Debatte, die meist unter dem Stichwort „gläserner Kunde“ bzw. „gläserner Bürger“ geführt wird.

Um die Chancen von RFID zu nutzen und gleichzeitig die Bedrohung für die Persönlichkeitssphäre zu minimieren, müssen die Grundsätze von Informationssicherheit und Datenschutzrecht bereits bei der Konzeption und Markteinführung von RFID-Anwendungen umgesetzt werden. Es gilt, RFID-Systeme zu entwickeln und einzusetzen, die auch den mittel- und langfristigen Anforderungen von Wirtschaft und Privatpersonen an Informationssicherheit[1] und Datenschutz[2] entsprechen. Nur so können zentrale Barrieren bei der wirtschaftlichen Nutzung der RFID-Technologie frühzeitig erkannt und so weit wie möglich vermieden werden.

Im Mittelpunkt dieses Beitrags stehen die Anwendungspotenziale von RFID-Systemen.

Was ist RFID-Technologie?

RFID-Systeme werden in vielfältigen Varianten angeboten. Trotz der großen Bandbreite ist jedes RFID-System durch drei Eigenschaften definiert: 1. Elektronische Identifikation: Das System ermöglicht eine eindeutige Kennzeichnung von Objekten durch elektronisch gespeicherte Daten. 2. Kontaktlose Datenübertra-

[1] Zu Fragen der Informationssicherheit vgl. die unter Mitwirkung der Autorinnen erstellte Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ (s. Kasten am Ende des Textes).
[2] Zu den spezifischen Risiken von RFID-Systemen im Bereich des Datenschutzes vgl. den Beitrag von Alexander Roßnagel in diesem Heft.

gung: Die Daten können zur Identifikation des Objekts drahtlos über einen Funkfrequenzkanal ausgelesen werden. 3. Senden auf Abruf (*on call*): Ein gekennzeichnetes Objekt sendet seine Daten nur dann, wenn ein dafür vorgesehenes Lesegerät diesen Vorgang abruft.

Ein RFID-System besteht aus zwei technischen Komponenten, einem Transponder und einem Lesegerät: Der Transponder – auch als *tag* bezeichnet – fungiert als Datenträger. Er wird an einem Objekt angebracht (z. B. an einer Ware oder einer Verpackung) bzw. in ein Objekt integriert (z. B. in eine Chipkarte) und kann kontaktlos über Funktechnologie ausgelesen und je nach Technologie neu beschrieben werden. Grundsätzlich setzt sich der Transponder aus einer integrierten Schaltung und einem Radiofrequenzmodul zusammen. Auf dem Transponder sind eine Identifikationsnummer und weitere Daten über den Transponder bzw. über das Objekt, mit dem dieser verbunden ist, gespeichert. Das Erfassungsgerät – im Folgenden als Lesegerät bezeichnet – besteht je nach eingesetzter Technologie aus einer Lese- bzw. einer Schreib-/Leseeinheit sowie aus einer Antenne. Das Lesegerät liest Daten vom Transponder und kann ihn anweisen, weitere Daten zu speichern. Weiterhin kontrolliert das Lesegerät die Qualität der Datenübermittlung. Die Lesegeräte sind mit einer zusätzlichen Schnittstelle ausgestattet, um die empfangenen Daten an ein anderes System (PC, Automatensteuerung) weiterzuleiten und dort weiter zu verarbeiten.

Sowohl Transponder als auch Lesegeräte werden in verschiedenen Ausführungen angeboten, die jeweils auf spezifische Anwendungsfelder und Einsatzbereiche ausgerichtet sind. Das Angebot an Lesegeräten kann grob in stationäre und mobile Ausführungen gegliedert werden, die teilweise auch für die Nutzung in rauen Umgebungen geeignet sind. Auch das Angebot an Transpondern ist vielfältig. Die Bauformen reichen vom Glas-Injektat über die elektrische Ohrenmarke bis hin zu Scheckkartenformaten, verschiedenen Scheibenbauformen sowie schlagfesten und bei bis zu 200 Grad Celsius hitzebeständigen Datenträgern für die Lackierstraßen in der Automobilindustrie.

RFID-Systeme nutzen unterschiedliche Frequenzen, vom Lang- bis zum Mikrowellenbereich. Ein weiteres Unterscheidungsmerkmal besteht in der zum Einsatz kommenden Speichertechnologie. Hier wird grundsätzlich zwischen *Read-only*- und *Read-write*-Systemen unterschieden. Auch die Art der Energieversorgung und die daraus resultierende Unterscheidung in aktive Transponder mit eigener Energiequelle bzw. passive Transponder, die durch das Lesegerät mit Energie versorgt werden, ist von grundlegender Bedeutung.

Aufgrund dieser Merkmale können Gruppen von RFID-Systemen gebildet und bezüglich der Leistungsfähigkeit ihrer jeweiligen Komponenten in *Low-End*-Systeme, Systeme mittlerer Leistungsfähigkeit und *High-End*-Systeme unterschieden werden. Eine weitere Gruppierung kann entsprechend ihrer jeweiligen Reichweite – also des maximal möglichen Abstandes zwischen Transponder und Lesegerät – erfolgen. Hier werden *Close-Coupling*-, *Remote-Coupling*- sowie *Long-Range*-Systeme unterschieden.

Anwendungspotenziale

RFID-Technologie lässt sich in nahezu allen Lebens- und Wirtschaftsbereichen anwenden. Theoretisch sind ihre Einsatzgebiete unbegrenzt (vgl. die *Abbildung*). Grundsätzlich geht es dabei immer um die Identifikation von Objekten. Bislang scheiterte eine weit verbreitete Nutzung der Technologie an den relativ hohen Kosten der Implementierung. Hierzu zählen Kosten für die Hardwarebeschaffung, die zusätzlichen Softwarekomponenten und – ein oft vernachlässigter Faktor – die Aufwendungen einer organisatorischen Anpassung an neue bzw. veränderte Geschäftsprozesse.[3]

Branchenübergreifend können die folgenden Anwendungsgebiete unterschieden werden:

– *Kennzeichnung von Objekten:* Praxisrelevante Anwendungen der kontaktlosen RFID-Identifikationssysteme in diesem Anwendungsgebiet finden sich beispielsweise in den Bereichen Tieridentifikation, Behälteridenti-

[3] Vgl. Progress Software, RFID-Integration – Brückenschlag vom Transponder zur Unternehmensanwendung, www.progress.com/worldwide/de/docs/rfid_whitepaper_de_gif.pdf (27. 11. 2005).

fikation und Abfallentsorgung. Aber auch die eindeutige Kennzeichnung von Waren und die Personenidentifikation zählen zu den relevanten Anwendungen.

– *Echtheitsprüfung von Dokumenten:* Weltweit werden Ansätze getestet, um RFID-Transponder in Personalausweise und Reisepässe zu integrieren. Das Ziel besteht darin, elektronische Fälschungsschutzmechanismen umzusetzen, erweiterte Echtheitsprüfungen zu ermöglichen und biometrische Merkmale – beispielsweise das Gesicht oder einen Fingerabdruck – in Ausweisen, etwa im Reisepass, zu speichern.

– *Instandhaltung und Reparatur, Rückrufaktionen:* RFID-Transponder werden von Unternehmen unterschiedlicher volkswirtschaftlicher Branchen zunehmend auch für automatisierte und individualisierte Instandhaltungs- und Reparaturdienste sowie für Rückrufaktionen genutzt.

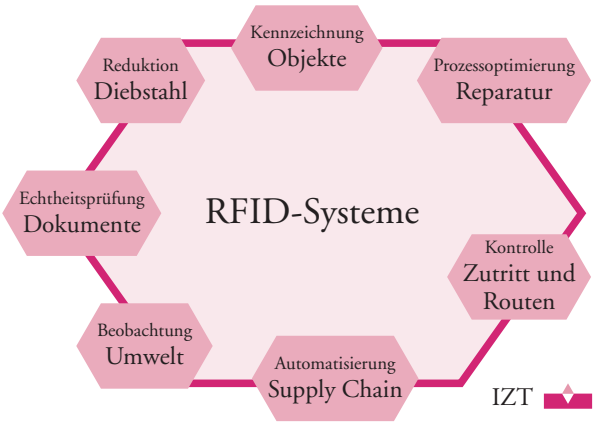
– *Zutritts- und Routenkontrollen:* Magnet- oder Chipkarten gehören bereits zum gesellschaftlichen Alltag. RFID-Systeme ermöglichen es heute, kontaktlos Daten zu erfassen und so die Leistungsmerkmale der traditionellen Kartenanwendungen zu erweitern. Das Anwendungsspektrum von RFID-Systemen reicht von der Wegfahrsperre im Auto über Zutrittssysteme beispielsweise in Betrieben.

– *Diebstahlsicherung und Reduktion von Verlustmengen:* Hier geht es vor allem um die Reduktion von Schwund und Diebstahl. RFID-Systeme dienen Fluggesellschaften nicht nur als Routenkontrolle, sondern helfen auch bei der Reduktion von Verlusten bzw. dem schnelleren Auffinden von verloren gegangenen Gepäckstücken.

– *Umweltmonitoring und Sensorik:* RFID-Systeme können in Verbindung mit hochgradig miniaturisierten, drahtlosen Sensoren dazu beitragen, die vielfältigen Phänomene der Umwelt mit bislang nicht möglicher Genauigkeit zu beobachten und Umweltbelastungen zu überwachen.

– *Supply-Chain-Management:* Transponder ermöglichen neben der reinen Identifikation von Objekten die Steuerung von Waren und Gütern in komplexen Systemen. Dabei wird die automatisierte Steuerung und Überwachung der Lieferkette in Zeiten von Lagerreduktionen und der Durchsetzung des *Just-in-time*-Prinzips zum entscheidenden Erfolgsfaktor.

Abbildung: Anwendungen von RFID-Systemen



Im Folgenden werden auf Basis der vorangestellten branchenübergreifenden Systematik einige ausgewählte Anwendungsbereiche von RFID-Systemen aufgezeigt.

Kennzeichnung von Objekten im Krankenhaus

Der Kostendruck im Gesundheitswesen und die zunehmenden rechtlichen Vorschriften zu einer immer besseren Leistungsdokumentation verlangen in der medizinischen Versorgung neue Lösungen. So hat beispielsweise die Gesundheitsstrukturreform Reorganisationsprozesse ausgelöst, die sich in neuen rechtlichen, organisatorischen und technologischen Konzepten niederschlagen (diagnosebezogene Fallgruppen, integrierte Versorgung).

Auf der Suche nach Innovationen, die den Arbeitsprozess in Kliniken optimieren und damit neben einer Qualitätssteigerung zu einer Kostensenkung führen, gewinnt die RFID-Technologie eine zunehmend bedeutendere Rolle. Auch wenn umfassende RFID-Lösungen für den Pharma- und Gesundheitssektor derzeit noch eher Vision als Realität sind, veranschaulicht die RFID-Technologie in verschiedenen Pilotprojekten technologische Innovationspotenziale, die neben der Authentifizierung auch die verschiedenen Möglichkeiten der Identifikation und der prozessimmanenten Qualitätssicherung umfassen. Die über den Transponder

mögliche Authentifizierung der Benutzer verfolgt im Gesundheitswesen zwei Funktionen: Die Eingabe der Daten kann eindeutig zurückverfolgt und die Dokumentare festgestellt werden. Zudem wird es durch die Authentifizierung möglich, die klinischen Daten rollenbasiert nach dem Informationsbedarf anzuzeigen. Auf den Transpondern können entsprechend dem Datenschutz Zugriffsrechte gespeichert werden. Sowohl Ärzte als auch examiniertes Pflegepersonal oder Zivildienstleistende werden mit diesen Transpondern z. B. am Stationsrechner individuell und automatisch angemeldet. Während die behandelnden Oberärzte kontrollierten Zugriff auf die gesamte Patientenakte erhalten, können die Pflegerinnen und Pfleger ausschließlich die für ihren Aufgabenbereich relevanten Teile einsehen. Die Authentifizierung ist nicht nur am Stationsrechner möglich, sondern auch bei der Zutrittskontrolle zu einzelnen Räumen oder ganzen Klinikbereichen, sodass sich die Tür zum Medikamentenraum oder dem Arztzimmer nur für Befugte öffnet.[4]

Für eine umfassende RFID-Lösung ist es erforderlich, auch die Patientinnen und Patienten mit einem Transponder auszustatten. Sie erhalten bei der Aufnahme in das Krankenhaus ein Armband, das sie durch alle Behandlungsstationen begleitet und auf dem per RFID-Chip der Verweis auf die Patientendaten im Krankenhaus-Informations-System (KIS) gespeichert ist. Die behandelnden Ärzte können bei der Visite mit einem mobilen Endgerät diesen *tag* auslesen und erhalten alle zum Patienten gehörenden Informationen. Auf diese Weise sollen Verwechslungen ausgeschlossen werden. Die Eindeutigkeit der Identifizierung kann lebenswichtig sein, wenn medikamentöse Unverträglichkeiten vorliegen oder bestimmte Dosierungen nicht über- oder unterschritten werden dürfen. Auch bei der Identifikation der Patienten vor einer Operation oder bei der Zuordnung von Pflege- und Betreuungsleistungen kann RFID die medizinische Versorgungsleistung unterstützen. Zudem können die Patientinnen und Patienten insofern Nutzen daraus ziehen, als sie an im Krankenhaus aufgestellten Informationsterminals individuelle Information abrufen können, beispielsweise darüber, wann die nächsten Behandlungstermine anstehen.[5]

Die RFID-basierte Identifikation im Gesundheitswesen kann sich neben der Identifikation von Personen auch auf die Identifikation von Material und medizinischen Geräten beziehen. So lässt sich mit aktiver Transpondertechnologie die Kühlkettenüberwachung verschiedener Medizinprodukte direkt im Prozess und ohne zusätzlichen Aufwand durchführen. So zeichnen beispielsweise an Blutbeuteln angebrachte aktive Transponder eventuelle Temperaturabweichungen auf und beugen so einer Schädigung des Patienten durch die Verabreichung verfallener Blutkonserven vor.[6] Auch die Inventarisierung und das Bestellwesen können deutlich vereinfacht werden: Transponder an allen medizinischen Geräten erleichtern die Verwaltung des abschreibbaren Bestandes. Die ausgelesenen Informationen geben den verantwortlichen Mitarbeiterinnen und Mitarbeitern aus der Krankenhausverwaltung einen genauen Überblick über das Inventar und die erforderlichen Anschaffungen.

Zutritts- und Routenkontrollen

Kontaktlose Zutrittssysteme haben sich bereits auf dem Markt durchgesetzt, wenn der Anbieter eine schnelle Identifikation von Einzelpersonen oder Gruppen unterstützen oder langwierige Kontrollverfahren verkürzen möchte. Dabei sind RFID-Systeme immer dann unter ökonomischen Kriterien attraktiv, wenn Personen Kontrollpunkte wiederholt passieren müssen. Als typisches und langjähriges Einsatzfeld haben sich elektronische Zugangskontrollsysteme an Urlaubszielen etabliert, die in der Regel mit einer digitalen „Geldbörse“ kombiniert werden.

So wurde in der österreichischen Region Nassfeld/Sonnenalpe in der Saison 1999/2000 eine RFID-Lösung umgesetzt, die eine Vielzahl touristischer Leistungsträger, wie Hotel-, Skihütten-, Skilift- oder Bergbahnbetreiber, einbezieht. Der Gast soll sich während des gesamten Aufenthalts „berührungs- und bar-

[4] Vgl. Optimierung von Betreuung und Wirtschaftlichkeit in Kliniken, www.n-tier.de/2_Produkte/2_1/2_1_2/hp_wireless_clinic_d.pdf (28. 11. 2005).

[5] Auf dieser Basis hat beispielsweise Arcor im Sana-Klinikum-Remscheid ein Pilotprojekt realisiert; vgl. http: // isis.de / RFID-Technologie _ und _ Koerpersen. 914.0.html (29. 11. 2005).

[6] Vgl. ACG Identification Technologies GmbH, www.acq.de (2. 7. 2004).

geldlos“ in der Region bewegen können. Mit einer Investitionsgesamtsumme von 715 000 Euro wurden achtzig Erfassungsgeräte, zehn Standardkassensysteme sowie fünfzig so genannte *Offsite Points Of Sale* – Ausgabestellen in Hotels- und Beherbergungsbetrieben, Skiverleihstellen und Skischulen – aufgebaut. Leistungen können auch über das Internet oder Mobilfunknetze gebucht und bei jeder Ausgabestelle auf dem Transponder gespeichert werden. Hierfür wurde ein regionales Funknetz aufgebaut, das in über vierzig Sende- und Empfangsstationen PCs mit einem Server verbindet, der Gästedaten zentral speichert.

Zum Einsatz kommen zwei unterschiedliche Typen von Transpondern im Kartenformat: Karten im Frequenzbereich von 122,8 kHz werden für Multiapplikationskarten genutzt (die auch als „Hotelschlüssel“ Verwendung finden), Karten im Frequenzbereich von 13,56 MHz finden als Skipass Verwendung. Die Speichergröße beträgt bei den eingesetzten 13,56-MHz-Karten 2 048 Bit. Die 13,56-MHz- Datenträger haben eine Up- und Downlink-Geschwindigkeit von bis zu 26 kbit pro Sekunde, die 122,8-kHz-Karten nur von drei kbit. Zwar erfüllt das Kartenformat die ISO-Norm 7810 und hat damit die typischen Chipkartengröße von 85,6 × 54 Millimeter. Das eigentliche RFID-System jedoch ist kein ISO-Datenträger. Der maximale Lese- und Schreibabstand beträgt jeweils 40 Zentimeter.

Antikollisionsverfahren sind zwar grundsätzlich möglich, wurden aufgrund einer „extremen Verschlechterung der Performance“ auf der Hardware-Seite im Erfassungsgerät aber nicht umgesetzt. Da Personen im Ski-Bereich einen durchschnittlichen Abstand von 80 Zentimetern halten, ist auch die Zahl der Transponder im Erkennungsbereich begrenzt. Um Fehler bei der Übertragung der Daten erkennen zu können, wird der *Cyclic Redundancy Check* eingesetzt. Auf den meisten der verwendeten Datenträger ist es möglich, mehrere Ebenen mit Berechtigungen zu belegen (z. B. Skipass auf der ersten Ebene, Hotelschlüssel auf der zweiten Ebene). Die Berechtigungen werden passwortgeschützt gespeichert. Eine Verschlüsselung der gespeicherten Daten erfolgt für jede einzelne Ebene.

Den Gästen wird bei Ankunft eine Karte für Zimmer, Skidepot, Skiverleih, Skipass und Geldbörse ausgestellt. Je nach den gebuchten Leistungen ermöglicht die Karte den Zutritt zu Skilifts, die Nutzung des Ski- und Boardverleihs sowie weiterer Angebote in der gesamten Region. Typischerweise erfolgt die Zutrittskontrolle über Schleusensysteme oder durch in Türrahmen installierte Zugangskontrollen. In Bars und Restaurants werden zu zahlende Beträge mit mobilen Erfassungsgeräten abgebucht. Die hohe Akzeptanz auf der Kundenseite begründen die Betreiber vor allem mit der Bequemlichkeit für den Kunden. Am Skilift entfällt das umständliche Suchen nach dem Skipass. Sofern die Karte verloren geht, kann sie schnell gesperrt und neu ausgestellt werden. Die Wartezeiten an den Verkaufsstellen werden verkürzt.

Für den Betreiber ergeben sich Einsparungspotenziale durch den schnelleren Zugang beispielsweise an Skilifts, durch den geringeren Personalaufwand bei der Zutrittskontrolle oder durch die schnellere Abwicklung von Zahlungsprozessen. Darauf aufbauend ermöglichen es die Daten des zentralen Marketingservers auch, das Leistungsangebot einzelner Leistungsträger oder des Zielgebietes insgesamt zu optimieren. Die Anwendung ermöglicht eine detaillierte Auswertung der Daten einzelner Kunden bzw. der Nachfrage nach Leistungen und des Umsatzvolumens insgesamt. Es entsteht eine große Menge personenbezogener Daten, die durchaus ein genaues Bild der Präferenzen und der Aufenthaltsorte bzw. der Pfade des Kunden während des Aufenthaltes in der Region abgeben können. An jeder Kasse kann eine genaue Routenverfolgung des Datenträgers erfolgen (benutzte Anlagen, zurückgelegte Höhenmeter). Diese Daten können für die Optimierung der Liftauslastung und die Infrastrukturplanung herangezogen werden. Gegenwärtig wird an Programmen gearbeitet, die diese Kundenströme grafisch darstellen sollen und damit auch dem Skigast eine Information über die Gebietsauslastung geben können.

Tickets für die Fußball-Weltmeisterschaft

Breites öffentliches Interesse weckt der Einsatz von RFID-Systemen im Zuge der Fußball-Weltmeisterschaft (WM) 2006 in Deutschland. So plant das Organisationskomitee des Deutschen Fußball-Bundes, alle Eintrittskarten mit Transpondern und die

Eintrittsschleusen der zwölf Stadien mit RFID-Lesegeräten auszustatten. Die Transponder werden eine Reichweite von zehn Zentimetern haben, das heißt, Besucherinnen und Besucher müssen die Tickets gezielt an die Lesegeräte heranführen. Im Rahmen des Confederation Cups im Sommer vergangenen Jahres wurde das System bereits im Stadion in Frankfurt/Main erfolgreich getestet.

Die Eintrittskarten werden zu 95 Prozent über das Internet nachgefragt. Am ersten Verkaufstag wurden rund acht Millionen Zugriffe auf den Server der WM 2006 verzeichnet. Das Interesse an Tickets übersteigt das Angebot deutlich. Das Organisationskomitee geht davon aus, dass dem Angebot von drei Millionen Eintrittskarten für die 64 Spiele eine Nachfrage in Höhe von etwa 50 Millionen Bestellungen – vergleichbar der letzten WM in Japan und Südkorea – gegenübersteht. Die Ticketpreise variieren zwischen 35 Euro für die günstigsten Karten in einem Vorrundenspiel und 100 bis maximal 600 Euro für das Endspiel.[7] Diese Zahlen verdeutlichen, dass Tickets für die WM ein knappes Gut sind. Trotzdem soll die Nachfrage nicht über den Preis, sondern über eine Verlosung der meisten Karten geregelt werden.[8]

Vor diesem Hintergrund bietet die RFID-Technologie einige Vorteile gegenüber anderen Zutrittssystemen:

– *Fälschungssicherheit:* Durch die Verifizierung der Käufer bei personalisierten Tickets mittels elektronischer Identifikation und kontaktloser Datenübertragung sollen die Besucher besser vor gefälschten Tickets geschützt werden: „Aus Sicherheitsgründen und zur Unterbindung des Schwarzhandels können Tickets nur mit Zustimmung des FIFA Fußball-Weltmeisterschaft 2006 Organisationskomitees Deutschland übertragen werden. Jedes Ticket wird auf den Namen des Bestellers oder den Namen des bei der Bestellung angegebenen Besuchers ausgestellt. Zu Kontrollzwecken ist entsprechend den Vorgaben der Veranstalter auch die Ausweis- oder Reisepassnummer im Formular anzugeben."[9] Beim Einlass werden die auf dem Transponder gespeicherten Daten mit der Datenbank des elektronischen Einlasssystems abgeglichen. In Zweifelsfällen müssen sich die Besucher ausweisen, um so einen Abgleich mit den bei der Registrierung gespeicherten Daten zu ermöglichen. Somit wird zwar kein absoluter Schutz vor Fälschungen realisiert, aber der unberechtigte Zutritt durch Fälschungen deutlich erschwert.

– *Neuausstellung im Verlustfall:* Bei Verlust eines Tickets können die Tickets ersetzt werden. Hierzu wird die eindeutige Identifikationsnummer des ursprünglichen Tickets gesperrt und eine neue Kennzeichnung vergeben.

– *Schneller Zutritt:* Im Berliner Olympiastadion sollen rund 75 000 Besucher in einem Zeitraum von zwei Stunden auch bei internationalen Großveranstaltungen und daraus resultierenden erhöhten Sicherheitsanforderungen auf Basis der RFID-Technologie die Zutrittskontrollen passieren können.

– *Internationale Sicherheitsauflagen:* Die FIFA hat die Vergabe der WM nach Deutschland mit Auflagen verbunden, beispielsweise, um das Risiko von Störungen und Bedrohungen durch Hooligans zu reduzieren. Die Tickets müssen personalisiert sein, eine „Fan-Trennung" muss gewährleistet und ein Abgleich der Stadionsverbotsdateien der wichtigsten teilnehmenden Staaten mit den Daten der Besucher durchgeführt werden. Um diese Personalisierung auch bei Zuschauern mit einer Vielzahl von Nationalitäten zu gewährleisten, erfasst die FIFA Pass- bzw. Personalausweisnummern. Darüber hinaus soll das RFID-System im Bedarfsfall auch „skalierbare" Sicherheitsvorkehrungen unterstützen. Nach der WM soll das Konzept von den Stadionbetreibern auch für die Bundesliga und andere Großveranstaltungen genutzt werden.[10]

Datenschützer und Datenschutzexperten erkennen an, dass bei der Fußball-Weltmeisterschaft eine „Sondersituation mit besonde-

[7] http://fifaworldcup.yahoo.com/06/de/tickets/prices.html (28. 11. 2005).

[8] Vgl. Willi Behr, Consultant Ticketing für die FIFA Fußball WM 2006, Vortrag anlässlich des Berliner Zukunftsgesprächs „Pervasive Computing – Chancen und Risiken einer neuen Technologie" des IZT – Institut für Zukunftsstudien und Technologiebewertung am 26. 10. 2005.

[9] Wie Anm. 7.

[10] Vgl. Ecin, Fußball-WM 2006 baut auf RFID, www.ecin.de/news/2004/01/16/06623 (27. 11. 2005).

ren Gefährdungen gegeben“ ist und dass sich das Organisationskomitee des DFB nicht den Auflagen der FIFA entziehen kann. Gleichzeitig weisen sie darauf hin, dass die RFID-Anwendung anlässlich der WM nicht ohne Anpassungsmaßnahmen im Rahmen der Bundesliga weitergeführt werden kann: So ist es in Deutschland unzulässig, Seriennummern der Personalausweise so zu nutzen, dass „mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist“.[11] Die Personalisierung der Tickets anlässlich der WM ist allein der besonderen Situation geschuldet und sollte eine Ausnahme darstellen.[12]

Logistiknetzwerke

Durch ihre Transparenz werden der RFID-Technologie hohe Chancen zugesprochen, logistische Prozessabläufe effizienter steuern zu können. Im Kern geht es um die Erschließung von Rationalisierungspotenzialen innerhalb unternehmensübergreifender Wertschöpfungsketten bzw. um größtmögliche Effizienz bei den übergreifenden Material-, Informations- und Geldmittelflüssen. Durch den Einsatz der RFID-Technologie können Produkte und Materialien in Echtzeit bis auf „Losgröße Eins“ über das gesamte Logistiknetzwerk hinweg verfolgt werden. Zudem ist eine Integration materieller betrieblicher Ressourcen mit bestehenden IT-Systemen möglich. An den Waren angebrachte Funkchips liefern Daten zu Produkten und ihren zeitlichen und räumlichen Bewegungen. Voraussetzungen sind die Definition gemeinsamer Standards sowie Lösungen, die Kosten und Nutzen adäquat auf die beteiligten Akteure der Wertschöpfungskette verteilen.

Den Untersuchungsergebnissen einer Studie von Booz Allen Hamilton und der Universität St. Gallen[13] zufolge rechnet sich der Einsatz von RFID in denjenigen Branchen, in denen aufgrund hoher Nachweispflichten höchste Prozesssicherheit erforderlich wird und zudem ein geschlossener Logistikkreislauf die Wiederverwendbarkeit der bislang noch teuren Chips sicherstellt, etwa in der Automobilindustrie. Offene Systeme, die heute Grundlage der Anwendung im Handel und der Konsumgüterindustrie sind, kommen laut Studie dagegen aufgrund der hohen Investitionen in Chips, Reader-Infrastruktur und Systemintegration noch nicht auf ein Kosten-Nutzen-Verhältnis.

Nichtsdestotrotz ist der Einzelhandel vor dem Hintergrund des intensivierten Wettbewerbsdrucks bestrebt, mithilfe der RFID-Technologie die Kosten in der Logistik flächendeckend zu senken. So bildet der METRO Group Future Store – eine Kooperation der METRO Group mit SAP, Intel und IBM sowie weiteren Partnerunternehmen aus den Bereichen Informationstechnologie und Konsumgüterindustrie – im nordrhein-westfälischen Rheinberg das Pilotprojekt für Supermärkte mit einem Bündel von technologischen Neuerungen, darunter die RFID-Identifikation. Eingesetzt wird sie derzeit hauptsächlich in der Lieferkette und im Lager des Future Stores zur Erprobung der Technologie. In weiteren Ausbaustufen soll der Einsatz ausgeweitet werden. Dieser Einsatz entspricht den Ergebnissen einer Studie, die für die Warenwirtschaft zwei zentrale Vorteile der RFID-Technologie benennt: die Reduzierung von Beständen und damit die Reduzierung von Lager- und Kapitalbindungskosten sowie die Reduzierung von Personalkosten in den Geschäften und Lagern.[14]

RFID-Systeme werden zunehmend auch zur logistischen Optimierung von Umschlagsplätzen wie Flughäfen oder Häfen genutzt. Auf dem Container-Terminal Altenwerder (CTA) des Hamburger Hafens werden bereits heute Verladung, Zwischenlagerung und Weitertransport der standardisierten Stahlboxen nahezu lückenlos von einem Computerprogramm organisiert. Sieben halbautomatische Brücken am Kai platzieren die Container präzise auf 35 fahrerlose Lastwa-

[11] Vgl. die datenschutzrechtlichen Bestimmungen des Gesetzes über Personalausweise (PAuswG).

[12] Vgl. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit, Vortrag anlässlich des Berliner Zukunftsgespräch „Pervasive Computing“ (Anm. 8).

[13] Vgl. Booz Allen Hamilton in Kooperation mit der Universität St. Gallen, RFID-Technologie: Neuer Innovationsmotor für Logistik und Industrie?, www.boozallen.de/content/downloads/5h_rfid.pdf (14. 12. 2005).

[14] Vgl. RFID spart dem deutschen Einzelhandel sechs Milliarden Euro pro Jahr: Nutzen für Händler – Kosten für Hersteller, Pressemitteilung vom 8. 3. 2004, www.atkearney.de/content/veroeffentlichungen/pressemitteilungen_detail.php/id/49046 (14. 11. 2005).

gen, die – über elektromagnetische Transponder geleitet – jeweils einen der elf Lagerblöcke ansteuern. Auf dem CTA-Gelände werden die Routen der automatischen Fahrzeuge über einen Computer geplant und gesteuert. Ein feinmaschiges Netz von im Asphalt integrierten Transpondern kontrolliert dabei ständig die Position der Fahrzeuge in dem 100 mal 1 400 Meter großen Areal zwischen Kai und Lager. Bis Ende 2005 sollten nahezu 12 000 Transponder im Asphalt versenkt sein und insgesamt 65 computergesteuerte, automatische Fahrzeuge mit stets aktualisierten Positionsdaten versorgen.[15]

Ausblick

In einzelnen Anwendungszusammenhängen konnte aufgezeigt werden, welche Vorteile der Einsatz von RFID-Systemen beispielsweise für das Gesundheitswesen oder für Logistik-Dienstleister bieten kann. Chancen lassen sich vor allem in Anwendungsgebieten und Branchen ausmachen, in denen Produktivitätsfortschritte durch eine verstärkte Automatisierung erzielt werden sollen.

Zu den Hauptwachstumsfaktoren für die weitere Verbreitung von RFID-Systemen zählen sinkende Preise und zunehmende gesetzliche Vorgaben. Aber auch die Kompatibilität und Interoperabilität sowie die Durchsetzung von einheitlichen Standards sind wesentliche Elemente, welche die Entwicklungsmöglichkeiten von RFID-Systemen maßgeblich beeinflussen. Positive Impulse gehen zudem von der zunehmenden Bekanntheit der RFID-Lösungen und vom Angebot kundenorientierter Lösungen aus.

Die Marktdaten und Berichte zum Einsatz von RFID-Systemen sind häufig punktuell, beziehen sich auf einzelne volkswirtschaftliche Sektoren und Anwendungsgebiete und geben keinen übergreifenden Marktüberblick. Die verwendeten Datengrundlagen, Erhebungsmethoden und Marktabgrenzungen sind sehr unterschiedlich, nicht immer transparent und daher nicht miteinander vergleichbar. Der Stand der Diffusion, der Umsätze und der Marktanteile von RFID-Systemen bleibt in der Folge national wie international unscharf. Ob sie zukünftig als Massentechnologie eingesetzt wird, hängt nicht zuletzt von den Erfolgen der laufenden Pilotprojekte von Pionieranwendern ab.

Auf der Grundlage von RFID-Systemen können Daten sehr viel leichter als bisher gesammelt werden. Im Zuge der weiteren Verbreitung der RFID-Technologie stellt sich die Frage, wer darüber bestimmen kann oder darf, ob und mit welchen Informationen elektronisch aufgewertete Dinge verknüpft werden. Um die Chancen von RFID zu nutzen und gleichzeitig die Bedrohung für die Persönlichkeitssphäre so gering wie möglich zu halten, müssen die Grundsätze eines zeitgemäßen Datenschutzrechts in RFID-Systemen bereits frühzeitig im Design-Prozess und in der Markteinführung umgesetzt werden. Hierzu zählen vor allem der Grundsatz der Datensparsamkeit und die schnellstmögliche Anonymisierung oder Verschlüsselung personenbezogener Daten. Dies gilt umso mehr, als politische und rechtliche Rahmenbedingungen im Zuge der fortschreitenden Globalisierung zunehmend schwieriger zu gestalten sind.

Internetempfehlungen der Autorinnen

Die Abschätzung der Chancen und Risiken des Einsatzes von RFID-Systemen mit Blick auf die Informationssicherheit und den Datenschutz und einem Überblick über die Anwendungspotenziale der RFID-Technologie ist Gegenstand der Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“. Sie wurde im Auftrag und in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer interdisziplinären Kooperation des Instituts für Zukunftsstudien und Technologiebewertung (IZT) und der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA) erstellt. Die Studie ist kostenlos in deutscher und englischer Sprache im Internetangebot des IZT unter www.izt.de/publikationen/andere_verlage erhältlich. Barrierefreie Fassungen stehen auf dem Server des BSI unter www.bsi.bund.de/fachthem/rfid/studie.htm bereit.

[15] Vgl. Torsten Engelhardt, Der Hamburger Hafen, in: Geo, (2003) 11; Thomas Koch, Automatik-Portalkrane im CTA-Containerlager, in: Hebezeuge und Fördermittel, 44 (2004) 11; Produktinformation der IND – Mobile Datensysteme GmbH, Willich: Transportaufträge via Datenfunk.

Patrick Radden Keefe

Der globale Lauschangriff

Im Februar 2003 unternahm die New Yorker Polizei hektische Anstrengungen, um die U-Bahn vor einem Terrorangriff zu schützen. Eine 16 000 Mann starke, in der Terrorbekämpfung besonders geschulte Einsatztruppe bezog überall in der Stadt Stellung. Die Behörden verstärkten die Patrouillen und Kontrollpunkte entlang der unzähligen unterirdischen Arterien, über welche die Pendler tagtäglich nach Manhattan hinein und wieder hinaus strömen. Polizeibeamte postierten sich an jedem einzelnen Eingang der 16 unter Wasser befindlichen U-Bahntunnel innerhalb und außerhalb der Stadtgrenzen und schritten die hunderte Meilen langen Bahnsteige mit Spürhunden, Geigerzählern und Gasmasken ab. Was hatte diese plötzliche Verstärkung der Sicherheitsmaßnahmen ausgelöst? Was hatte das New York Police Department aufgeschreckt? Es war nur ein einziges Wort in einer abgehörten Unterhaltung zwischen Terrorverdächtigen: „Underground".

Patrick Radden Keefe
geb. 1976; Yale Law School; Projektleiter am World Policy Institute, New York.
54 Sidney Place, Brooklyn, NY 11201, USA.
Psrkeefe@gmail.com

Ganz harmlos hat sich der Begriff *chatter* in unseren Wortschatz eingeschlichen, „Geplapper" bzw. „Geschnatter" – ein kleines Wort, belanglos in seinen Assoziationen. Über Nacht erhielt der Begriff jedoch eine neue und beunruhigende Bedeutung. Inzwischen ist das elektronische „Geschnatter" eines bestimmten Tages gleichsam zu einer Art Panikbarometer geworden. Wie aus den meteorologischen Hinweisen, die einer Wettervorhersage zugrunde liegen, leiten wir aus *chatter* ab, ob sich ein Unheil zusammenbraut, ob wir uns im Alarmzustand oder sogar im höchsten Alarmzustand befinden; *chatter* vermittelt uns die exakte akustische Nuance für den Bedrohungsindex des nächsten Tages.

Aus welch eigentümlichem Gebräu leiten unsere Regierungen das Gefühl der Bedrohung ab, das wir an einem bestimmten Tag empfinden sollen? Die meisten Menschen machen sich davon keine Vorstellung. Aus aufgefangenem *chatter*, so hörten wir, gehe hervor, dass der Irak unter Saddam Hussein Massenvernichtungswaffen herstelle. Zudem sei *chatter* den Terrorangriffen vom 11. September 2001 vorausgegangen. In den Wochen vor einer Katastrophe, so wird uns gesagt, bilde sich ein bestimmtes Muster heraus. Vor dem 11. September, den Bombenanschlägen in Bali im Oktober 2002 und den Selbstmordattentaten in Riad im November 2003 sei *chatter* ganz plötzlich zu einem regelrechten Crescendo fremder Stimmen angestiegen. Dann Stille. Dann Desaster. Wir wissen nur sehr wenig über die Terroristen der Al-Qaida, über ihren perversen Fundamentalismus, die tödliche Verbindung einer rückwärts gewandten Philosophie mit einer zukunftsgerichteten Technologie, über ihre schwer fassbare, virusähnliche Organisationsstruktur. Der verräterische, sich verändernde Rhythmus aber ist uns inzwischen bekannt: erst *chatter*, dann Stille, dann Angriff. Elektronisches Geschnatter ist zum alles überragenden, geisterhaften Phänomen der ersten Jahre des 21. Jahrhunderts geworden. Wer redet da? Wer hört zu? Wie vollzieht sich dieses Zuhören? Und vielleicht am wichtigsten: Wie vertrauenswürdig ist *chatter* als Vorbote künftigen Unheils?

Das Echelon-Netzwerk

Eine verbreitete Verschwörungstheorie besagt Folgendes: Die USA sind das beherrschende Mitglied eines geheimen Netzwerks, das gemeinsam mit vier anderen anglophonen Mächten – Großbritannien, Kanada, Australien und Neuseeland – die Gespräche von Menschen, den *chatter*, rund um den Globus belauscht. Der Pakt zwischen diesen Ländern wurde vor einem halben Jahrhundert geschlossen, in einem Dokument, das so geheim ist, dass seine Existenz von keiner der beteiligten Regierungen zugegeben worden ist:

Übersetzung aus dem Amerikanischen von Susanne Laux, Königswinter.
Der Beitrag beruht auf dem Buch des Autors, Chatter. Dispatches from the Secret World of Global Eavesdropping, New York 2005. Dort finden sich auch alle Quellenhinweise.

UKUSA. Das von den genannten Staaten geknüpfte Netzwerk zeichnet täglich Milliarden von Telefonaten, E-Mails, Faxen und Telexen auf und verbreitet sie über eine Reihe automatischer Kanäle an interessierte Gruppen in den fünf Ländern. Auf diese Art bespitzeln die USA ihre NATO-Verbündeten und Großbritannien seine Verbündeten in der EU: Das Netzwerk hat jede andere Bindung, etwa Loyalität und Zugehörigkeit, ersetzt. Jedes Land hat Gesetze gegen die Bespitzelung seiner eigenen Bürger erlassen, nicht aber dagegen, dass seine Verbündeten diese Bürger ausspionieren – und so wirft Großbritannien auf Betreiben der USA gelegentlich ein Auge auf Einzelpersonen in den Vereinigten Staaten, im stillschweigenden Einvernehmen darüber, dass die Briten jeden auftauchenden Leckerbissen auch über den Tisch reichen.

Die Technologie, die diese fünf Länder zum Abhören der Kommunikation nutzen, ist höchst ausgeklügelt. Unser kleiner Wortschatz zur Beschreibung von „lauschen" strotzt vor Anachronismen. In seinen „Commentaries on the Laws of England" (1765/69) definierte Sir William Blackstone einen Lauscher (*eavesdropper*) als jemanden, der „hinter Mauern, unter Fenstern oder unter den Dachgesimsen eines Hauses Gespräche mithört und daraus verleumderische und boshafte Geschichten strickt". Der Begriff Lauscher lässt noch immer an Subjekte denken, die sich wie in den Theaterstücken Shakespeares und Molières hinter Wandschirmen verstecken. Selbst *wiretap*, das Anzapfen eines Kabels, hat etwas Kurioses: Viele Abhörmaßnahmen im vergangenen Jahrhundert hatten nichts damit zu tun, ein Kabel anzuzapfen, sondern damit, Signale ganz einfach aus der Luft zu „pflücken".

Signals intelligence, im Polit- und Agentenjargon auch *Sigint* genannt, ist die wenig bekannte Bezeichnung, die von den modernen Lauschern für das Abhören und Auswerten elektronischer Signale verwendet wird. Lauschen ist zu einem besonders innovativen Spiel geworden, seit es Abhörstationen gibt, die Gespräche aufzeichnen, die über Satelliten- und Mikrowellenantennen verbreitet werden, seit es Spionagesatelliten gibt, die meilenweit über uns im Weltraum schweben und sich in Radiofrequenzen auf dem Boden einklinken, seit es unhörbare und unsichtbare Internetwanzen gibt, die sich parasitengleich an den Knotenpunkten und Kreuzungen der Datenautobahn festsetzen.

Obwohl viele Amerikaner gar nicht wissen, dass sie existiert, ist die National Security Agency (NSA) – jene Behörde, die für elektronische Lauschaktionen zuständig ist – größer als CIA und FBI zusammen. Diese beiden besser bekannten Geheimdienste sind im Vergleich zur NSA belanglos. Während die CIA ungefähr 20 000 Beschäftigte und ein Budget von annähernd drei Milliarden US-Dollar aufweist, verfügt die NSA über mehr als 60 000 Beschäftigte, die über den gesamten Globus verstreut sind, und ihr Budget wird auf jährlich sechs Milliarden US-Dollar geschätzt. Bei der amerikanisch-britischen Zusammenarbeit bei *Sigint* verfügt die NSA über sehr viel engere Beziehungen zum britischen Abhördienst (*Government Communications Headquarters*, GCHQ) als zur amerikanischen CIA. Das anglophone Netzwerk, so heißt es, hört absolut alles, und doch ist seine Existenz ein nahezu perfekt gehütetes Geheimnis – manchmal selbst für die gesetzgebenden Körperschaften jener Länder, die es betreiben. Der Codename dieses Netzwerks lautet Echelon.

Wie jede gute Verschwörungstheorie lässt sich auch die eben aufgezeigte nicht falsifizieren. Es lässt sich weder beweisen, dass sie der Realität entspricht, noch lässt sie sich widerlegen. Genährt wird die Theorie durch offizielle Dementis und Weigerungen, sie zu kommentieren. Sie ist das paranoide Märchen des Internetzeitalters. Ihre Verbreitung verlief so epidemisch, wie Geschichten dies online zu tun pflegen; die Verschwörungstheorie spielt mit den Ängsten, die jene Menschen hegen, die große Mengen an persönlichen Informationen in ein Netzwerk einspeisen, ohne zu wissen, wie sicher der Transfer dieser Informationen ist. Gleichzeitig aber scheint die Theorie – trotz der angeblich grenzenlosen Natur des Internets – in Europa eine größere Anhängerschaft gefunden zu haben als in den USA. Wenn Meldungen über Echelon überhaupt ins Bewusstsein der Amerikaner vorgedrungen sind, dann nicht etwa über Tageszeitungen oder die Abendnachrichten, sondern eher über eine alarmistische Fernseh- und Romanfolklore.

Eigentümlich an dieser besonderen Verschwörungstheorie ist: Zumindest in groben Zügen scheint sie zuzutreffen. Vor einigen Jahren hat das Europäische Parlament einen Untersuchungsausschuss eingesetzt, um die Wahrheit über Echelon herauszufinden. Wird es dazu benutzt, die Europäer auszuspionieren? Der Ausschuss hat ein ganzes Jahr damit verbracht, Nachforschungen zu betreiben und Interviews durchzuführen und stand am Ende doch mit leeren Händen da; seine Mitglieder konnten keinen Beweis erbringen, und die Geheimdienste waren zu keiner Zusammenarbeit bereit. Zumindest eine Zeit lang gelang es der NSA, jenen Nimbus der Unscheinbarkeit bewahren, der in den USA den Witz aufkommen ließ, das Kürzel stehe für „Never Say Anything", oder einfacher noch: „No Such Agency".

Eine kleine Gruppe von Journalisten und Forschern in Großbritannien, Dänemark, Neuseeland und den USA begann, um die Welt zu reisen und „Horchposten" zu identifizieren, jene Einrichtungen des Weltraumzeitalters, die zum Abhören von über Mikrowellen und Satelliten übermittelten Gesprächen genutzt werden und mit denen der Planet seit dem Kalten Krieg regelrecht übersät ist. Sie führten Interviews mit ehemaligen „Lauschern" und durchforsteten öffentliche, nicht länger als geheim eingestufte Dokumente, Unternehmensbeschreibungen, Tagesordnungen von Konferenzen, Patente – alles, was einen Hinweis auf die Existenz und die Konturen des Echelon-Netzwerks geben könnte.

Eine interessante Wende ergab sich, als vor ungefähr einem Jahr ein amerikanischer Journalist des Internet-Magazins „Slate.com" ein Routineinterview mit Admiral Bobby Ray Inman führte, dem ehemaligen Direktor der NSA. Der Fragesteller, A. L. Bardach, hatte den Admiral zum Irak und zum Anti-Terror-Krieg befragt, als er abrupt das Thema wechselte und auf Echelon zu sprechen kam. Inman wurde vielleicht überrumpelt, doch er bestätigte bereitwillig dessen Existenz. Er sprach von dem Programm in der Vergangenheitsform, ganz so, als ob es mit den Jahren von neueren Technologien und Codenamen abgelöst worden sei, nicht zuletzt, nachdem die Medien über das System berichtet hatten, und nach der eingehenden Untersuchung in Brüssel. Er bestätigte, dass Echelon entwickelt worden sei, um die in Europa und anderswo geführte Kommunikation abzuhören. „Tatsächlich beschränkte es sich nicht nur auf Europa", so Inman, „es hatte weltweite Ausmaße." Eine der umstrittensten Behauptungen des Untersuchungsausschusses im EU-Parlament lag darin, dass Echelon zur Wirtschafts- und Industriespionage genutzt worden sei – was US-Offizielle vehement verneinten. Inman hingegen beeilte sich, klarzustellen, dass Echelons „tatsächliche Bedeutung wirtschaftlicher Natur war".

Das Ende der Geheimagenten

Ungeachtet der Andeutungen Inmans, Echelon werde nicht mehr eingesetzt, sind die amerikanischen Geheimdienste derzeit in einer neuen technologischen Seifenblase gefangen. Während in den späten neunziger Jahren jeder College-Schüler mit einem eilig zusammengeschusterten Geschäftsplan für ein „dot-com"-Unternehmen große Mengen an Risikokapital anlocken konnte, sind es heute die neuen Technologien zur nationalen Sicherheit, die – egal wie teuer sie sind oder wie unklug – lukrative Verträge ermöglichen. Der teuerste Einzelposten im amerikanischen Geheimdienstetat des Jahres 2005 ist die jüngste Generation eines „Stealth"-Spionagesatelliten, der die Erde unentdeckt im Weltraum umkreisen und Ziele auf dem Boden fotografieren soll. Die „Tarnkappen"-Qualitäten dieses Satelliten mit dem Codenamen „Misty" sind jedoch zweifelhaft – als die erste Generation 1990 in den Orbit geschickt wurde, wurde sie fast sofort entdeckt, und das nicht etwa vom sowjetischen Geheimdienst, sondern von Hobbyastronomen in Schottland und Frankreich. Der Preis für dieses von Lockheed-Martin entwickelte „Superding", bei dem mehrere amerikanische Senatoren Vorbehalte angemeldet haben, liegt bei 9,5 Milliarden US-Dollar. Mit diesem Geld, so ein Offizieller aus dem Pentagon, könne man eine zweite CIA aufbauen.

Dies sieht nach einer verfehlten Prioritätensetzung aus, es stimmt aber mit den jüngsten Vorlieben der amerikanischen Geheimdienste überein. Die USA verfügen derzeit über weniger als 2 000 weltweit operierende Geheimagenten, jedoch über mehr als 30 000 Lauscher. Alle drei Stunden sammeln die Satelliten der NSA Informationen vom Umfang

der Library of Congress in Washington. Doch Amerika leidet unter einem derart dramatischen Mangel an Sprachwissenschaftlern, welche die Milliarden abgehörten Kommunikationsschnipsel auswerten könnten, dass Ende 2005 ein gewaltiger Rückstau von aufgefangenen Gesprächen zwischen Terrorverdächtigen aufgelaufen war, die noch übersetzt werden mussten – ein Rückstand von rund 8 000 Stunden.

So sieht das undurchschaubare Gesicht der amerikanischen Geheimdienste im 21. Jahrhundert aus. Das Ende des Kalten Krieges veränderte grundlegend die Art der geheimdienstlichen Tätigkeit. Die Dezentralisierung der Bedrohung, die von der Sowjetunion ausgegangen war, führte zusammen mit einem geschrumpften Verteidigungshaushalt, neuem Optimismus und einer niedrigeren Toleranzschwelle der USA für Opfer und Verluste zu einer erheblichen Reduzierung der Spione vor Ort. Verschwunden sind die in einen Trenchcoat gekleideten Kalten Krieger der Romane von John le Carré, die CIA-Spione, die als Vorhut der Geheimdienste ausgesandt wurden, um aus den Botschaften heraus die Opposition zu infiltrieren oder um Maulwürfe und Doppelagenten zu rekrutieren und bei all dem ihr Leben riskierten. Gegen Ende des Kalten Krieges war die operative Aufklärungsarbeit (*Human intelligence* bzw. *Humint* im Geheimdienstjargon) bereits im Niedergang begriffen; sie verlor in den neunziger Jahren weiter an Bedeutung.

Die Amerikaner waren nicht länger gewillt, das Leben von Geheimagenten in Ländern aufs Spiel zu setzen, die angesichts des Verschwindens der Sowjetunion keine strategische Rolle mehr spielten, oder das Leben von Soldaten an Orten wie Mogadischu oder Sarajewo zu gefährden. Sie investierten stattdessen kräftig in neue Technologien der Kriegführung und der Nachrichtenbeschaffung durch eine Überwachung aus der Ferne. Die Regierungen unter George Bush sen. und Bill Clinton machten in einer Reihe von Konflikten deutlich, dass die USA von nun an, wo immer dies möglich schien, den Einsatz von Geräten dem von Menschen vorzogen.

Dieser Trend war nicht neu. Seit den siebziger Jahren hatte der Gedanke an Gewicht gewonnen, dass mit dem Fortschritt der Technik der vor Ort operierende Geheimagent überflüssig werden könnte. CIA-Direktor Stansfield Turner traf sich zweimal pro Woche mit Präsident Jimmy Carter, um ihn über die verschiedenen Formen der Nachrichtenbeschaffung durch die USA zu informieren. Beide hielten den „traditionellen Agenten“ im Grunde genommen für antiquiert. Nur wenige Wochen vor den Terrorangriffen des 11. September veröffentlichte ein früherer CIA-Agent namens Reuel Marc Gerecht im „Atlantic Monthly“ einen Artikel, in dem er die „risikoscheue bürokratische Natur der Behörde“ beklagte und durchblicken ließ, dass diese Einstellung dazu geführt habe, dass es im Nahen Osten keine wirkungsvolle operative Aufklärung mehr gebe. Seine Schlussfolgerung lautete: „Solange die Soldaten Osama Bin Ladens nicht selbst in ein Konsulat oder eine Botschaft der USA kommen, stehen die Chancen eines Abwehroffiziers der CIA schlecht, überhaupt jemals einen solchen zu Gesicht zu bekommen.“

Das UKUSA-Abkommen

Als Henry Lewis Stimson 1929 von Präsident Herbert Hoover zum Außenminister ernannt wurde und erfuhr, dass amerikanische Codeknacker die Kommunikation der britischen, französischen, italienischen und japanischen Diplomaten abgehört und gelesen hatten, empörte er sich: „Gentlemen lesen keine Post von anderen Leuten“ – so sein überlieferter Ausspruch. Ungeachtet dieser Pietät aber waren Abhöraktionen im 20. Jahrhundert sowohl in Kriegs- als auch in Friedenszeiten ein wichtiger, wenn auch verschleierter Teil der Arbeit des amerikanischen Geheimdienstapparates.

Nachdem die Alliierten im Zweiten Weltkrieg nicht zuletzt aufgrund ihrer geheimen Kooperation bei der Entschlüsselung elektronischer Signale siegreich waren, entschlossen sie sich, diese fruchtbare Zusammenarbeit in Friedenszeiten fortzuführen. Am 12. September 1945, kurz nach der japanischen Kapitulation, unterzeichnete Präsident Harry Truman ein streng geheimes, aus einem Satz bestehendes Memorandum, das den Kriegs- und den Marineminister ermächtigte, „die Zusammenarbeit auf dem Feld der Nachrichtenbeschaffung zwischen der amerikanischen und der britischen Armee und Marine fortzusetzen, diese Zusammenarbeit im besten Interesse

der Vereinigten Staaten auszuweiten, zu modifizieren oder aber zu beenden".

Warum sollte die enge Zusammenarbeit in Friedenszeiten fortgesetzt werden? Zum Teil ist dies mit den Befürchtungen der Alliierten bezüglich der Sicherheitslage zu erklären, vor allem angesichts des Aufstiegs der Sowjetunion unter Stalin. Die Amerikaner befürchteten, dass sie nicht alle in der Welt versendeten Signale abfangen könnten. Die Horchposten ihrer Marine waren vor allem auf den Pazifik ausgerichtet und befanden sich in Guam, Samoa und Okinawa; ihre Erfassung des Atlantiks war auf den Süden konzentriert, auf Puerto Rico, Brasilien und die Region um den Panama-Kanal. Währenddessen verfügten die Briten über Abhörstationen im Nordatlantik, in der Nordsee und im Mittelmeer, im Roten Meer und im Indischen Ozean bis hin zum Südpazifik. Die Briten hatten zudem Zugang zu den Abhörstationen in Kanada, Australien, Neuseeland und Südafrika. Zum Teil war es auf ihre Aufgabenverteilung während des Krieges zurückzuführen, dass die USA und Großbritannien jeweils das besaßen, was dem anderen fehlte. Nur durch eine fortgesetzte Zusammenarbeit glaubten sie, jene globale Allwissenheit erwerben zu können, die in einer unsicheren Nachkriegszeit angeraten zu sein schien.

So kam es, dass der amerikanische Dechiffrierexperte William Friedman im Februar 1946 für zwei Monate zu Geheimverhandlungen nach England reiste. Sir Stewart Menzies, Leiter des britischen Militärgeheimdienstes MI6, war ermächtigt worden, auch im Auftrag Kanadas und Australiens zu verhandeln. Im Verlauf dieser Gespräche kristallisierte sich ein Dokument heraus, das in seiner endgültigen Version rund 25 Seiten umfassen sollte. In den archivierten Aufzeichnungen fehlt ein kurzer, aber folgenreicher Abschnitt: die eingangs genannte Geheimdienstvereinbarung zwischen Großbritannien und den USA, bekannt als „United Kingdom–USA Communications Intelligence Agreement", abgekürzt UKUSA. Ihre bloße Existenz unterliegt noch immer strenger Geheimhaltung, und Kopien des vollständigen Dokuments lagern in Tresoren in den Hauptstädten der fünf Signatarstaaten.

Die Vereinbarung zerschnitt die Erde in fünf Verantwortungsbereiche, um die Arbeit des globalen Lauschangriffs zu verteilen. In der Anfangsphase der 1947 zunächst nur von den USA und Großbritannien unterzeichneten Vereinbarung sollte der britische GCHQ seine Horchposten in Großbritannien und auf Zypern zur Bespitzelung Westeuropas und des Nahen Ostens nutzen. Im folgenden Jahr traten Kanada, Australien und Neuseeland dem Abkommen als „zweite Partei" bei. Eine weitere Gruppe „dritter Parteien" wie Japan, Südkorea und verschiedene NATO-Verbündete kamen in den folgenden Jahren hinzu.

Entscheidend war eine Abstufung des Abkommens, das keineswegs gleichberechtigte Vertragsparteien vorsah. Großbritannien und die USA sind „erste Parteien". Aber selbst diese Einteilung ist irreführend. Während des Krieges mag sich Großbritannien noch mehr oder weniger auf Augenhöhe mit den USA befunden haben, in den ersten Nachkriegsjahren aber und mit Beginn des Kalten Krieges, als die USA ihre Position als Supermacht festigten, wurde der Status der Briten Schritt für Schritt zurückgestuft. Ein ehemaliger NSA-Beamter hat dies folgendermaßen ausgedrückt: „(Alle) Informationen gelangen in die USA, die USA aber erwidern diese Weitergabe von Information an die anderen Mächte nicht in vollem Umfang." Tatsächlich geben die meisten amerikanischen Stützpunkte in anderen Ländern ihre gesammelten Nachrichten direkt an das Hauptquartier der NSA in Fort Meade in Maryland weiter. Von dort erhalten die anderen Mächte die Informationen. Obwohl also die verbündeten Staaten die gigantischen Ohren der NSA beherbergen, hören sie nur das, was Amerika sie hören lassen möchte.

Eine Schwierigkeit, ein solches Netzwerk geheim zu halten, besteht darin, dass die Stützpunkte überall zu finden und nicht gerade unauffällig sind. In Menwith Hill, mitten im Yorkshire Moor in Nordengland, sprießen Dutzende eierschalenfarbene „Kuppeln" aus der Erde. Sie sehen aus wie riesige Golfbälle. Jede dieser weißen Kuppeln beherbergt eine sehr empfindliche Satellitenschüssel, schützt diese vor den Elementen und verhüllt deren Ausrichtung. Offiziell ist Menwith Hill ein Stützpunkt der britischen Luftwaffe, in Wirklichkeit aber Arbeitsplatz für 1 400 Amerikaner – Ingenieure, Mathematiker, Dechiffrier-Experten, Linguisten, Analytiker. Jede nur vorstellbare Berufsrichtung wird für eine Abhöraktion globaler Güte benötigt.

Menwith Hill ist der größte Horchposten, der strahlendste Stern in einer Konstellation großer und kleiner Stützpunkte, deren Mikrowellenantennen und Satellitenschüsseln in den Himmel weisen: Bad Aibling in Deutschland, Misawa in Japan, Akrotiri auf Zypern, Guantanamo Bay auf Kuba und Pine Gap mitten im Herzen Australiens. Trotz ihrer Lage in fremden Ländern werden diese Stützpunkte in der Regel mit vollem Einverständnis der nationalen Regierungen von den Amerikanern betrieben. Die meisten der Staaten, die diese Stützpunkte zur Verfügung stellen, haben dafür überzeugende Gründe: ein enges militärisches Bündnis mit den USA mit dem stillschweigenden oder ausdrücklichen Versprechen militärischen Schutzes, sollte er jemals benötigt werden, ferner ein gewisser Austausch von geheimdienstlichen Erkenntnissen, bei dem der „Mieter" jede wertvolle Erkenntnis an die „vemietende" Regierung weitergibt. Oft spielt auch Geld die entscheidende Rolle: Um einen Stützpunkt in einem strategischen Teil der Welt aufrechtzuerhalten, an dem eine Vielzahl elektronischer Signale empfangen werden kann, sind die USA bereit, sehr großzügige Mieten zu zahlen.

Selbst die engsten Verbündeten der Amerikaner im Geheimdienstbereich – Großbritannien, Kanada, Australien und Neuseeland – haben nur begrenzten Einfluss auf die Vorgänge auf diesen Stützpunkten. Sicher befinden sich Vertreter der jeweiligen Länderregierungen innerhalb des Zauns, und manchmal spielen sie auch eine wichtige Rolle: Sie helfen bei der Steuerung und der Wartung der zur Nachrichtenbeschaffung nötigen Ausrüstung oder bei der Analyse der Ergebnisse. Genauso oft aber ist die Rolle dieser Regierungsvertreter lediglich symbolischer Natur. Ein britischer Offizier, der auf dem Stützpunkt der Royal Air Force in Edzell, einem amerikanischen Horchposten südlich von Aberdeen in Schottland, beschäftigt war, erklärte in den siebziger Jahren in einem Gerichtsverfahren: „Ich bin der einzige britische Beamte auf dem Stützpunkt. Ich weiß nicht, was dort geschieht. (...) Ich bin völlig isoliert, meine US-Kollegen reden nicht mit mir."

Im Vorfeld des Irak-Krieges

Es muss nicht hervorgehoben werden, dass der globale Lauschangriff eine ernste Bedrohung für die Privatsphäre Einzelner darstellt. In der Vergangenheit haben die Geheimdienste beständig versichert, dass sie zwar Menschen rund um den Globus abhören, nicht aber Amerikaner. Im vergangenen Jahr jedoch, während der Anhörungen des neuen UN-Botschafters der USA, John Bolton, vor dem amerikanischen Senat stellte sich heraus, dass diesem während seiner Zeit als Unterstaatssekretär im State Department mehrfach Berichte über Gespräche von US-Bürgern vorgelegt wurden. Offiziell ist die NSA bei der Anlage derartiger Berichte verpflichtet, die Namen der Betroffenen durch die allgemeine Bezeichnung „US-Bürger" zu ersetzen, um deren Privatsphäre zu schützen. Auf Rückfrage Boltons allerdings versorgte ihn die NSA kurzerhand mit den entsprechenden Klarnamen. Nach eingehenden Recherchen enthüllte das Magazin „Newsweek", dass die Offenlegung der Namen von US-Bürgern in der Tat allgemeine, wenn auch nicht offen zugegebene Praxis in Washington sei, und dass die NSA während eines Zeitraums von 18 Monaten in den Jahren 2003 bis 2004 etwas mehr als 10 000 Namen auf diese Art und Weise preisgegeben habe.

Dies hätte nach den Enthüllungen des Jahres 2004, dass die NSA den britischen Abhördienst GCHQ um Unterstützung bei der Bespitzelung von Mitgliedern des UN-Sicherheitsrates in New York gebeten hatte, nicht wirklich überraschen sollen. Seinerzeit sollten deren Stimmverhalten bezüglich des Resolutionsentwurfes zum Irak beeinflusst und sie davon überzeugt werden, dass weitere Waffeninspektionen keine weise Lösung seien. Ein streng geheimes Memorandum eines NSA-Beschäftigten namens Frank Koza vom 31. Januar 2003 las sich wie folgt: „Wie Sie wohl schon gehört haben, bereitet die Behörde eine große Aktion vor, die sich insbesondere auf die Mitglieder des UN-Sicherheitsrates (UNSC) richtet (ausgenommen natürlich die USA und Großbritannien), um Erkenntnisse darüber zu gewinnen, wie die Mitglieder in der gegenwärtigen Debatte um die Irak-Resolution reagieren werden, über Abstimmungspläne hinsichtlich verwandter Resolutionen, darüber, welche Verhandlungspositionen und welche Bündnisse sie möglicherweise einzunehmen gedenken etc. – die ganze Bandbreite der Informationen, die amerikanischen Entscheidungsträgern einen Vorsprung verschaffen könnten bei der Herbeiführung

von Resultaten, die amerikanischen Zielen gelegen kommen und um Überraschungen auszuschalten."

Das Memorandum, das von Katherine Gunn, einer jungen chinesischen Übersetzerin beim GCHQ, publik gemacht wurde, enthüllte, dass die USA und Großbritannien wenig Bedenken hatten, eine ganze Reihe von Gesetzen und vertraglichen Verpflichtungen gegen das Ausspionieren im eigenen Land und von Diplomaten zu verletzen, um eine Zustimmung zur Invasion des Irak zu erreichen. Weiter hieß es in dem Memorandum, dass eine „Flut" von Abhörmaßnahmen, die sich gegen Diplomaten aus den so genannten „mittleren sechs" Ländern richte, nötig sei – jene Delegationen im Sicherheitsrat, die sich bezüglich ihrer Stimmabgabe bei der bevorstehenden Irak-Resolution noch unsicher waren: Angola, Kamerun, Chile, Mexiko, Guinea und Pakistan. Koza führte weiter aus, dass die NSA auch um die Weitergabe von Informationen über die „nicht im Sicherheitsrat angestellten Überlegungen, Debatten und Stimmverhalten" gebeten habe und dass „diese Aktion (zumindest mit diesem besonderen Fokus) möglicherweise Mitte nächster Woche, nach der Rede des Außenministers im Sicherheitsrat am 5. Februar, ihren Höhepunkt" erreichen werde.

Wie nie zuvor hat dieser Vorfall die engen Arbeitsbeziehungen zwischen den USA und Großbritannien in Fragen der Nachrichtenbeschaffung enthüllt. Nach Aussage von Katherine Gunn war es für das GCHQ nicht ungewöhnlich, derartige Anfragen von einem Angehörigen eines, wie sich am Ende herausstellte, ausländischen Geheimdienstes zu erhalten. Der Vorfall zeigte ferner, dass mit Geheimhaltung auch strafloses Handeln einher geht – Geheimdienste, die über enorme Möglichkeiten verfügen, neigen unbeobachtet vom kontrollierenden Blick parlamentarischer Körperschaften oder der Medien dazu, sich rücksichtslos über nationales und internationales Recht hinwegzusetzen.

Die Illusion globaler Allwissenheit

Nun könnte man einwenden, den Geheimdiensten könne getrost unterstellt werden, dass sie vom Bestreben geleitet werden, ihren Job gut zu erledigen, die nationalen Interessen ihrer Länder zu fördern und künftige Terrorangriffe zu verhindern. Eine typisch amerikanische Einstellung, die in den Jahren seit dem 11. September 2001 häufig geäußert wurde, lautet: „Warum sollte ich mich um meine Privatsphäre oder um Antiabhör-Gesetze sorgen, wenn ich nichts Verbotenes tue? Schließlich dient diese Form der Abhörtechnologie unser aller Sicherheit."

In unsicheren Zeiten scheint jeder Konflikt zwischen den Bedingungen der Freiheit und der Sicherheit zugunsten letzterer entschieden zu werden. Das größte Problem der elektronischen Nachrichtenbeschaffung ist, dass sie mit so viel Geheimniskrämerei betrieben wird. Wir sind nicht in der Lage, ihre Wirksamkeit einschätzen zu können. In vielerlei Hinsicht müssen wir uns nicht mit der Frage aufhalten, wie bedrohlich diese Technologie für die Privatsphäre oder bürgerliche Freiheiten sein kann, wenn wir uns nicht zuvor einer wichtigeren, der entscheidenden Frage zuwenden: Funktionieren diese Technologien überhaupt? Wenn viel mehr Kommunikation abgehört wird, als gesichtet und übersetzt werden kann, wäre *Sigint*, das Abhören und Auswerten elektronischer Signale, nicht nur eine Gefährdung der bürgerlichen Freiheiten, sondern eine gigantische Verschwendung von Ressourcen und finanziellen Mitteln.

Schließlich haben sich auch die meisten Versprechungen der „dot-com-Blase" als Illusion erwiesen. Die meisten jener ehrgeizigen Geschäftspläne kurz vor der Jahrtausendwende warfen kaum greifbare Resultate ab. Ist es nicht möglich, dass die Investitionen in die Überwachungstechnologie eine ähnliche Enttäuschung garantieren? Und, wenn das zutrifft: Ist es nicht möglich, dass sich die Vorstellung von der globalen Allwissenheit durch Abhörtechnologie ebenso als Illusion erweisen wird? Könnte nicht auch diese Blase platzen?

Es ließe sich mit Recht behaupten, dass dies schon längst geschehen ist. Der Höhepunkt der amerikanischen Begeisterung über die neue Geheimdiensttechnologie traf mit der „großen" Abhöraktion zusammen, um die Frank Koza von der NSA nachgesucht hatte. Am 5. Februar 2003 trat US-Außenminister Colin Powell an das Podium des Weltsicherheitsrates und erklärte: „Vor wenigen Wochen erst haben wir ein Gespräch zwi-

schen zwei Befehlshabern des Zweiten Korps der Republikanischen Garden im Irak abgehört, bei dem einer der beiden dem anderen eine Anweisung gibt." Begleitet von Übersetzungen ließ Powell daraufhin eine arabische Tonbandaufnahme abspielen. „Sie werden im Verlauf des Gesprächs hören, was der eine dem anderen mitteilen möchte", so Powell weiter, „er will durch Wiederholungen sichergehen, dass der andere Kerl alles auch deutlich versteht, so dass es niedergeschrieben und vollständig verstanden werden konnte. Hören Sie zu."

Der Raum war erfüllt von zwei arabischen Männerstimmen, die sich ein von Störgeräuschen verzerrtes Frage-und-Antwort-Spiel lieferten. Die Übersetzung lautete: Oberst: „Captain Ibrahim?" – Captain: „Ich höre Sie, Sir." – Oberst: „Streichen Sie das." – Captain: „Streichen Sie das [wiederholt die Anweisungen]." – Oberst: „Den Begriff." – Captain: „Den Begriff." – Oberst: „Nervengas." – Captain: „Nervengas." – Oberst: „Wo auch immer es auftaucht." – Captain: „Wo auch immer es auftaucht." – Oberst: „In den Anweisungen über Funk." – Captain: „In den Anweisungen." – Oberst: „Über Funk." – Captain: „Über Funk."

„Warum wiederholt er das auf diese Weise?", fragte Powell, nachdem das Band abgespielt worden war. „Warum drängt er so beharrlich darauf, dass dies verstanden worden ist? Und warum verweist er so eindringlich auf die Anweisungen über Funk? Weil der höhere Offizier besorgt ist, dass jemand dies abhören könnte." Powell machte eine Pause, um seine Worte wirken zu lassen: „In der Tat", so Powell weiter, „jemand hat gelauscht." Im scharfen Tonfall des Anklägers erklärte Powell, dass die Unterhaltung die „zurückhaltende Einschätzung" der Bush-Regierung bestätige, nach der die Irakis über einen Vorrat von 100 bis 500 Tonnen chemischer Kampfstoffe verfügten.

Dies taten sie aber nicht. Acht Monate nach Powells Vorführung, am 2. Oktober 2003, teilte der Waffenexperte David Kay, der von George Tenet ernannte Chef des CIA-Überwachungsteams im Irak, den Mitgliedern des Geheimdienstausschusses des amerikanischen Kongresses mit, dass er keinen Beweis für die Existenz von chemischen Kampfstoffen vorlegen könne. Kay ging sogar so weit zu sagen, dass es nach bestem Wissen des Überwachungsteams seit 1991 kein Chemiewaffenprogramm im Irak mehr gegeben habe. Die abgehörten Telefongespräche hatten nur scheinbar einen schlüssigen Beweis für Powells Behauptungen geliefert.

Hier liegt die Achillesferse von Echelon und des monströsen weltweiten Überwachungsapparates: Gespräche sind eine derart veränderliche, mehrdeutige Angelegenheit, so beladen mit Täuschungen und Doppelzüngigkeit, Schönfärberei und Verschleierung, dass man die Welt beim Zuhören wie durch eine geschwärzte Glasscherbe sieht. Es ist eine Sache, eine Nachricht aufzufangen, hingegen eine ganz andere zu verstehen, was sie bedeutet – selbst unter der Annahme, dass alles andere nach Plan verläuft, dass ein Gespräch abgehört, pünktlich übersetzt, in seiner wörtlichen Bedeutung verstanden und an die zuständigen Stellen weitergegeben und verbreitet wird. Gespräche nach Hinweisen auf künftige Ereignisse zu durchsuchen ist so willkürlich und unsicher wie Kaffeesatzleserei.

Es war eine der merkwürdigen Ironien des Sommers 2001, dass sich nur eine Woche nach der Annahme des Echelon-Abschlussberichts im Europäischen Parlament, der die Umrisse eines angeblich allmächtigen angloamerikanischen Überwachungsnetzes aufzeichnete, ein massiver und verheerender Angriff ereignete, der keinerlei Eingang in die Ohren der damit befassten Geheimdienste gefunden hatte. Dem System, das nach Aussage eines ehemaligen kanadischen Horchpostens „alles erfasst, was zu jedem beliebigen Zeitpunkt weltweit ausgestrahlt wird (. . .). Jeden Quadratzentimeter", ist es nicht gelungen, auch nur die Vorboten einer Warnung aufzufangen. Nach diesem doppelten Versagen der Geheimdienste im Vorfeld des 11. September 2001 und im andauernden Irak-Konflikt lässt sich kaum mehr bestreiten, dass der globale Lauschangriff seine Zukunft bereits hinter sich hat. Er ist gescheitert.

Dennis Mocigemba

Computer und Nachhaltigkeit

Am 22. April, dem weltweiten Aktionstag für die Erde (Earth Day) des Jahres 2005, versammelten sich Aktivisten verschiedener Nichtregierungsorganisationen (NGOs) zu einer *unApple*-Kampagne vor dem Hauptquartier der Firma Apple Computers in Cupertino, Kalifornien. Mit ihrem Protest wollten sie das Unternehmen ermahnen, soziale und ökologische Standards einzuhalten. Zwar feierte die Computerfirma in den vergangenen Quartalen einen Rekordgewinn nach dem nächsten. Im Vergleich zu den Konkurrenten Hewlett Packard und Dell, so der Kernvorwurf der Aktivisten, sei Apple allerdings ein Nachzügler im Umgang mit Elektroschrott und produziere weiterhin Produkte mit hohen Anteilen umwelt- und gesundheitsschädigender Schwermetalle.

Dennis Mocigemba
Dr. phil., geb. 1975; Postdoctoral Fellow an der International University Bremen, Jacobs Center for Lifelong Learning, Communication Science. Postfach 750 561, 28725 Bremen.
d.mocigemba@iu-bremen.de

In Europa, insbesondere in Deutschland, wurde für die Giftstoff- und Elektroschrottdebatte vergleichsweise schnell ein institutioneller Rahmen geschaffen: Im Januar 2003 erließ die Europäische Union Richtlinien zur Reduzierung gefährlicher Stoffe in Neugeräten und zum Umgang mit Altgeräten. Als einer der ersten Mitgliedstaaten setzte Deutschland beide Richtlinien mit dem am 23. März 2005 in Kraft getretenen „Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten“ (ElektroG) in nationales Recht um.

Die Giftstoff- und Elektroschrottdebatte dient als anschauliches und aktuelles Beispiel für einen Ausgleich zwischen ökonomischen Interessen und ökologischen sowie sozialen Forderungen unterschiedlicher Akteure innerhalb der Welt der Informationstechnologie (IT). Ähnlich geartete Debatten haben die IT-Branche in der Vergangenheit stark geprägt, ja gespalten: Schlagworte wie Freie Software, Digitale Spaltung, Softwarepatente und Open Source bergen seit Jahren, teilweise seit Jahrzehnten ein starkes Konfliktpotenzial. Die mit diesen Schlagworten belegten Debatten wurden bisher selten mit dem Begriff Nachhaltigkeit assoziiert. Das dürfte vornehmlich daran liegen, dass ihr Schwerpunkt meist auf dem Ausgleich ökonomischer und sozialer Interessen lag. Ökologische Aspekte spielten höchstens im Hinblick auf Gesundheitsaspekte und den Verbraucherschutz eine Rolle.

Der Begriff der Nachhaltigkeit stammt ursprünglich aus der Forstwirtschaft. Mittlerweile hat er eine bemerkenswerte Karriere als politisches Konzept hinter sich und sickert seit einigen Jahren verstärkt in den alltäglichen Sprachgebrauch. Die Folge sind konkurrierende Begriffsdefinitionen und eine wachsende Ambiguität. Gemäß dem 1987 veröffentlichten Zukunftsbericht der Weltkommission für Umwelt und Entwicklung (*Brundtland-Report*) wird Nachhaltigkeit hier als ein auf die Ausgewogenheit ökonomischer, ökologischer und sozialer Interessen gerichteter Aushandlungsprozess verschiedener Akteure und Interessengruppen verstanden.[1]

Einige dieser Aushandlungsprozesse werden im Folgenden skizziert und auf ihren normativen Grundgedanken reduziert: die Vermittlung zwischen ökonomischen, sozialen und ökologischen Interessen. Eine solche Reduktion öffnet die Diskurse der IT-Welt für Außenstehende und erlaubt eine breitere Vermittlung dessen, worum es in den teilweise sehr technischen Debatten jeweils geht. Dadurch wird eine breite Partizipation an der Diskussion der Frage ermöglicht, in welcher Welt wir mit welcher Technik leben wollen. Diese Partizipation ist die notwendige Voraussetzung für jegliche Form nachhaltiger Entwicklung.

[1] Vgl. World Commission for Environment and Development (WCED), Our Common Future, New York 1987.

Digitale Spaltung

Die Geschichte des Computers als technisches Artefakt und Produkt ist geprägt von polarisierenden Debatten über seine Sozialverträglichkeit. Noch Ende der sechziger Jahre waren Computer in der öffentlichen Meinung stark umstritten. Man betrachtete sie als entmenschlichenden Faktor in Arbeitsprozessen und in der Gesellschaft generell. In den USA sah sie die Bewegung gegen den Vietnamkrieg zudem als Mittel der Kriegführung an und stellte sie in einen politischen und sozialen Kontext.

Mit zunehmender Verbreitung stieg der Computer allmählich zum politischen Symbol auf. Viel einflussreicher als die diffusen Befürchtungen einer skeptischen Öffentlichkeit waren hierbei allerdings soziale Bewegungen und ihre Forderungen aus Kreisen, die an der Entwicklung und Verbreitung von Hard- und Software maßgeblich beteiligt waren. Pioniere wie Joseph Carl Robnett Licklider und Douglas Engelbart priesen mit griffigen Visionen und Schlagworten („Mensch-Computer-Symbiose“ bzw. „Intelligenzverstärkung“) die Nützlichkeit der Computertechnologie auch im Privaten, einem Bereich, in dem sich diese für breite Teile der Bevölkerung zu jener Zeit noch nicht erkennen ließ.

Diese zunächst unpolitischen Visionen wurden bald mit politischen und sozialen Forderungen aufgeladen: „Computer Power to the People!“, lautete in den siebziger Jahren das Motto der als „Computer Liberation“ firmierenden Bewegung. „By Computer Lib. I mean simply: making people freer through computers“,[12] beschrieb Ted Nelson, der vielleicht profilierteste Aktivist jener Tage, das Ziel. Nelson warnte vor einer gesellschaftlichen Spaltung durch die ungleiche Verteilung von Computern und den damit einhergehenden ungleichen Chancen, von ihnen zu profitieren. Plakativ und provokativ sprach er von zwei sich voneinander entfernenden Kulturen, den *Nerds* und den *Fluffies*; die einen hatten Zugriff auf und Kenntnisse über die neue Technologie, den anderen blieb sie verwehrt.

[12] Theodor Holm Nelson, Computer Lib/Dream Machines, (Eigenverlag) 1974, S. 70.

Die starke Verbreitung von Personalcomputern (PCs) und des Zugangs zum Internet in der industrialisierten Welt lässt derartige Forderungen als Relikte vergangener Zeiten erscheinen. Doch ist die Debatte um die Verfügungsmacht und den Zugang zu IT-Technologie auch heute noch aktuell. Die gesellschaftliche Spaltung vollzieht sich allerdings nicht mehr vornehmlich zwischen technikbegeisterten *Nerds* und skeptischen *Fluffies*. Zwar sprechen deutsche Initiativen wie „Schulen ans Netz“ oder verschiedene Seniorennetze gezielt vermeintlich benachteiligte soziale Gruppen an. Eine viel tiefere digitale Spaltung jedoch vollzieht sich im globalen Maßstab zwischen industrialisierter Welt und Entwicklungsländern.

Die digitale Spaltung (*digital divide*) war Anlass für den ersten UN-Weltgipfel zur Informationsgesellschaft (WSIS) 2003 in Genf. Dort wurden Grundsätze und ein Aktionsplan zur Gestaltung einer weltweiten Informationsgesellschaft formuliert. Der zweite Gipfel dieser Art fand im November 2005 in Tunis statt. Er wurde dominiert von Diskussionen über die freie Meinungsäußerung im Internet, die Öffnung der Märkte in ärmeren Ländern für die Informationstechnologien und die Verwaltung des Internets (*internet governance*).

Usability und Barrierefreiheit

Eine andere Diskussion hat ebenfalls mit der Frage zu tun, wie die Chancen und Vorteile des Computers als Werkzeug und Arbeitsmittel sozialverträglich verteilt werden können, und konzentriert sich somit ebenfalls auf den Ausgleich zwischen ökonomischen und sozialen Interessen. Es handelt sich um den im Bereich der Qualitätssicherung angesiedelten Diskurs über die Anpassung von Computersystemen an die Bedürfnisse verschiedener Nutzergruppen. Unter Nutzern versteht man hier Personen, die den Computer für ihre Zwecke benutzen (müssen), ohne über ein detailliertes Verständnis seiner technischen Funktionsweise zu verfügen.

Usability (Nutzungsqualität bzw. Gebrauchstauglichkeit) und Barrierefreiheit sind zwei zentrale Termini dieser Diskussion. Hinter ihnen steckt die soziale Forderung an Softwareentwickler, Computersysteme an die

Bedürfnisse ihrer Nutzer anzupassen, um niemandem systematisch die Möglichkeit zu rauben, von Computersystemen zu profitieren. Auch soll niemand gezwungen werden, seine Lebens- und Arbeitsweisen technischen Notwendigkeiten zu unterwerfen. Allein der technische Fortschritt und der Einzug des Computers in fast alle Lebensbereiche dürfe nicht dazu führen, dass Personen, beispielsweise aufgrund mangelnder technischer Kompetenz oder Begeisterung, sozial benachteiligt würden. Computerprogramme sollten deshalb in hohem Maße gebrauchstauglich sein. *Usability* ist ein mittlerweile international genormtes Konzept (ISO 9241:11), nach dem Software aufgabenangemessen, selbstbeschreibungsfähig, erwartungskonform, steuerbar, fehlertolerant, lernförderlich und individualisierbar sein muss (ISO 9241:10).

Das Konzept der Barrierefreiheit legt das Hauptaugenmerk auf Personen mit Behinderungen (z. B. Sehbehinderte) und ist vor allem im Zusammenhang mit dem Internet bekannt geworden. Als barrierefrei bezeichnet man Internetangebote, die sowohl von Menschen mit Behinderung oder mit altersbedingten Einschränkungen als auch von automatischen Suchprogrammen uneingeschränkt genutzt werden können. Da dies nur selten vollständig erreicht wird, spricht man auch von barrierearmen Produkten und Angeboten. Auch der Terminus Barrierefreiheit, der meist mit *accessibility* übersetzt wird, zielt auf sozialen Ausgleich: Potenziell benachteiligte Personen sollen von der Computernutzung gleichermaßen profitieren können.

Usability wird oft als Qualitätsmerkmal eines Produkts verstanden, dessen Umsetzung sich auch ökonomisch rentiert.[3] Barrierefreiheit hingegen wird von Softwareentwicklern eher aufgrund gesetzlicher Verpflichtungen angestrebt oder aufgrund ihrer solidarischen Wertorientierung, selten aus ökonomischem Nutzenkalkül.

Elektroschrott und Ressourcenverbrauch

Wie eingangs angedeutet, sehen sich Hardwareproduzenten seit einiger Zeit zunehmend nicht nur mit sozialen, sondern auch mit ökologischen Forderungen konfrontiert. So gründete sich im Jahr 2001 in den USA die Computer Take Back Campaign (CTBC) mit dem Ziel, Hersteller von Hardware zu einem verantwortlichen Umgang mit Altgeräten, zur Mitgestaltung von Gesetzesinitiativen, Formulierung von Recyclingzielen und Etablierung von Rücknahmesystemen zu bewegen. Mit der jährlich veröffentlichten Computer Report Card versucht die CTBC, eine Währung zu etablieren, die Auskunft über die Rücknahmeaktivitäten eines Produzenten im Vergleich zu seinen Verkaufsmengen erlaubt. Die Inaktivität der großen Hersteller führt laut CTBC derzeit häufig dazu, dass Elektroschrott über unseriöse Recyclingfirmen in Entwicklungsländer verschifft und dort nicht fachgerecht entsorgt wird, nicht selten durch (schlecht bezahlte und ungenügend geschützte) Häftlinge in Gefängnissen. Schätzungen zufolge exportieren allein die USA bis zu 80 Prozent ihres Elektroschrotts nach Indien, China und Pakistan, wo Computer ohne Schutzvorrichtungen zerlegt oder offen verbrannt werden. Elektroschrott verursacht heute das weltweit am schnellsten wachsende Abfallproblem.

Problematisch ist das Recycling von Computer-Hardware, weil sich nur etwa fünf bis zehn Prozent eines Geräts wiederverwerten lassen. Der Rest lässt sich durch Verbrennung allenfalls in Form von Energie wieder nutzen. Bis zu zehn Prozent des Gesamtvolumens eines PCs müssen endgelagert werden.[4] Während Rücknahmesysteme bei anderen Elektrogeräten bereits gut funktionieren, ist die Quote fachgerecht recycelter Computer noch sehr gering. Das eingangs erwähnte ElektroG ist der Versuch des deutschen Gesetzgebers, die Produktverantwortung durch die Hersteller zu erhöhen, indem diese die Entsorgungskosten der Altgeräte tragen müssen. Damit soll ein ökonomischer Anreiz für eine umweltschonende Produktionsweise geschaffen werden.

Neben der Frage nach der Wiederverwertung von Elektroschrott ist aus ökologischer, aber auch aus wirtschaftlicher Perspektive

[3] Vgl. Jakob Nielsen, Usability Engineering, San Francisco 1994, S. 2 ff.

[4] Vgl. Thomas Beschorner et al., Institutionalisierung von Nachhaltigkeit. Eine vergleichende Untersuchung der organisationalen Bedürfnisfelder Bauen & Wohnen, Mobilität und Information & Kommunikation, Berlin 2005, S. 198.

vor allem die Frage nach dem Ressourcenverbrauch von Informationstechnologie interessant: Während der Energieverbrauch in der Produktionsphase von Hardware, insbesondere von Prozessoren, weiterhin steigt, sinkt der Energieverbrauch in der Nutzungsphase seit Jahren stetig. Entsprechende Siegel wie etwa das EPA-Siegel der US-Umweltbehörde oder das schwedische TCO 95 sollen den Verbraucher auf besonders energiesparende und somit langfristig günstigere Hardwarekomponenten hinweisen und nachhaltige Konsumprozesse anregen.

Die Optimierung der Hardware führt zu erhöhter Effizienz. Einzelne Geräte oder Komponenten verrichten bei gleichbleibendem Energieverbrauch höhere Leistungen. Dennoch werden mit solchen Effizienzsteigerungen absolut betrachtet nicht zwingend Ressourcen eingespart. Das Phänomen, dass Effizienzsteigerungen einzelner Geräte oder Komponenten durch eine wachsende Verbreitung und Nutzung dieser Geräte ausgeglichen oder sogar überkompensiert werden, nennt sich *rebound effect*. Hoffnungen darauf, Informationstechnologie würde bestimmte energieintensive Praktiken des Alltags wie beispielsweise den Papierverbrauch reduzieren, werden immer wieder enttäuscht. Langfristig werden Effizienzsteigerungen nur dort zu einer im Sinne von Nachhaltigkeit erwünschten Wirkung führen, wo sie mit Suffizienzstrategien einhergehen, die z. B. die absolute Gütermenge begrenzen oder auf eine energiesparende Gerätenutzung abzielen, eingebettet in Lebensstile und alltägliche Praktiken.[5]

Freie Software und Open Source

Im Jahr 1976 verkauften Bill Gates und Paul Allen einen BASIC-Interpreter, einen „Übersetzer" der Computersprache BASIC, für den damals sehr populären *Altair*-Heimcomputer. Dieser Verkauf rief Aufsehen und Empörung hervor, weil er gegen die damals unter Programmierern dominierende Hacker-Ethik verstieß.[6] Diese garantierte Softwareentwicklern freien Zugriff auf und uneingeschränktes Teilen von Information. In einem offenen Brief verteidigte Gates sein Vorgehen und stellte seine Arbeit als Programmierer mit jener der Hardwareentwickler auf eine Stufe. Er bezichtigte Entwickler, die Software frei teilten, des Diebstahls und warf ihnen vor, die Entwicklung guter Software zu erschweren. Der Brief löste heftige Debatten aus, und der Vorfall ging als *Software Flap* in die Geschichte ein.

Mit dem Aufstieg der Softwareproduktion zur Industrie verloren ethisch-moralische und soziale Forderungen gegenüber ökonomischen Interessen zunehmend an Bedeutung, bis der Informatiker Richard Stallman 1985 die Free Software Foundation (FSF), eine gemeinnützige Organisation zur Förderung und Produktion Freier Software, gründete. Sein Konzept umfasst vorrangig Fragen zur Lizenzierung von Software und die Forderung nach einem für jedermann zugänglichen Quelltext. Bekanntheit erlangte Stallman durch das GNU-Projekt.[7] Dieses verfolgt das Ziel, ein freies Betriebssystem zu etablieren und die Hacker-Ethik wiederzubeleben. Motivation schöpfte Stallman dabei vornehmlich aus seiner Arbeit an einem Texteditor namens *Emacs*, der von vielen Entwicklern gemeinsam erarbeitet und ständig verbessert wurde. Die Nutzungsbedingungen von *Emacs* sahen vor, dass jeder das Programm frei anwenden und seinen Bedürfnissen (z. B. durch das Schreiben von Zusatzfunktionen) anpassen darf, solange er diese Änderungen der Gemeinschaft von Nutzern (*Emacs Commune*) mitteilt: „Emacs was more than a single software programm. It was a social contract."[8] Stallman sprach häufig von einer *Church of Emacs* und den moralischen Verpflichtungen der Entwicklergemeinde.

Neben einigen heute weit verbreiteten Entwicklerwerkzeugen (z. B. Debugger, Compiler) ist die *GNU General Public License* (GNU GPL) aus dem Jahr 1989 das wahrscheinlich wertvollste Resultat des GNU-Projekts. Diese versucht ganz im Geiste alter Hackerzeiten am Massachusetts Institute of Technology (MIT) oder in der *Emacs Commune* das Teilen von Information und das ge-

[5] Vgl. Lorenz M. Hilty/Thomas F. Ruddy, Towards a Sustainable Information Society, in: Informatik/Informatique, 4 (2000), S. 8.
[6] Vgl. Steven Levy, Hackers. Heroes of the Computer Revolution, London 1994, S. 39 ff.
[7] GNU ist ein rekursives Akronym und steht für „GNU is not Unix".
[8] Sam Williams, Free as in Freedom. Richard Stallman's Crusade for Free Software, Sebastopol 2002, S. 85.

meinschaftliche Entwickeln zu forcieren. Sie garantiert die Partizipation am Entwicklungsprozess von Software nach den Fähigkeiten des Einzelnen und nicht nach Firmenzugehörigkeit. Die GNU GPL hatte einschneidende Wirkung auf den Entwicklungsprozess von Software: 1991 veröffentlichte Linus Torvalds das dem GNU-Projekt lange fehlende Herz eines freien Betriebssystems, den Kernel namens *Linux*. Er stellte diesen unter die GNU GPL. Der Siegeszug von Linux ist seither auch ein Siegeszug der GNU GPL und somit eines alternativen, egalitären, offenen und freieren Entwicklungsmodells von Software.

Trotz seines Votums für die GNU GPL distanzierte sich Torvalds stets vehement von den ethisch-moralischen Ansprüchen der FSF. Er bezeichnete Stallman als „religiösen Fanatiker" und grenzte sich wiederholt von dessen sozialen und politischen Forderungen ab: „Ich muss zugeben, dass mir die gesellschaftspolitischen Fragen, die Stallman so am Herzen lagen (. . .), kaum bewusst waren (. . .). Mich interessierte die Technik, nicht die Politik."[9] 1998 spaltete sich ein Teil der Free-Software-Bewegung von Stallman ab und führte den Begriff Open Source ein. Dieser unterscheidet sich nur geringfügig von Stallmans Free Software-Konzept. Open-Source-Anhänger kritisieren an der Free-Software-Bewegung vornehmlich deren starke ideologische Ausrichtung und die Überbewertung ethisch-moralischer gegenüber technischen Diskussionen. Derartige Spannungen innerhalb dieses alternativen Modells der Softwareentwicklung führten zu zwei unterschiedlichen Schulen. Eric Raymond brachte dies mit einer Metapher auf den Punkt: Den Ansatz Stallmans und der FSF verglich er mit dem Bau einer Kathedrale, den Ansatz der Open-Source-Bewegung mit einem Basar: Während der Kathedralenbau einen großen Entwurf benötigt und hehre moralische Werte die treibende Kraft hinter dem Bau darstellen, existiert der Basar aufgrund einer Vielzahl unterschiedlicher Einzelinteressen, die keines ideologischen Überbaus bedürfen.[10] Das Ziel, den Entwicklungsprozess zu öffnen und zu demokratisieren, ist beiden Ansätzen gemein, bezüglich Motivation und Mittel hingegen unterscheiden sie sich.

Mit seinem Engagement für Freie Software und der daraus hervorgegangenen Open-Source-Bewegung hat Stallman die wahrscheinlich bedeutendste Nachhaltigkeitsdebatte innerhalb der IT-Welt angestoßen und soziale Aspekte, zum Beispiel bezüglich egalitärer Zugangs- und Nutzungschancen, sowohl im Produktions- als auch im Nutzungsprozess von Software fest verankert.

Softwarepatente

Ein weiteres Spannungsfeld, das als Nachhaltigkeitsdiskurs betrachtet werden kann, ist die Debatte um das Recycling von Software. Mit der Ablehnung der EU-Richtlinie zur Patentierbarkeit „computerimplementierter Erfindungen" im Juli 2005 durch das Europäische Parlament ist diese Diskussion auch in Deutschland wieder entflammt. Eine allgemein akzeptierte Definition für Softwarepatente hat sich hier bisher nicht durchsetzen können. Vor allem die Frage nach der Technizität und Trivialität einer Software (-Erfindung) steht hier im Mittelpunkt. Anders als traditionelle Patente, die sich auf technische Erfindungen beschränken, beziehen sich Softwarepatente oft auf Ideen. Von Lizenzvereinbarungen, die das Urheberrecht schützen und immer für bestimmte Implementierungen gelten, unterscheiden sich Softwarepatente dadurch, dass sie nicht einzelne Programme, sondern ganze Verfahrensklassen schützen. In den USA ist die Patentierung von Software sehr verbreitet, was zu dem Phänomen der Trivialpatente geführt hat: So besitzt z. B. amazon.com ein Patent auf den Einkauf per Mausklick (*One-Click-Shopping*), die Firma Adobe auf die Darstellung eines Karteikartenreiters am Bildschirm und Apple auf eine Methode zur Stapelung mehrerer virtueller Dokumente auf dem Desktop.

Neben der Legalität ist auch die Legitimität der Softwarepatentierung sehr umstritten. Kritiker der Softwarepatentierung wie Stallman oder der gemeinnützige Förderverein für eine Freie Informationelle Infrastruktur sehen in Softwarepatenten eine Einschränkung der Programmierfreiheit. Sie befürchten vor allem eine Benachteiligung kleiner und

[9] Linus Torvalds/David Diamond, Just for Fun. Wie ein Freak die Computerwelt revolutionierte, München 2002, S. 66.

[10] Vgl. Eric Raymond, The Cathedral and The Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary. Revised and expanded edition, Sebastopol 2001.

mittelständischer Unternehmen. Große Unternehmen könnten, so die Sorge, die Patente kleiner Unternehmen schlicht ignorieren, bis diese die Gerichtskosten zur Durchsetzung ihrer Patente nicht mehr aufbringen. Auch wird eine Zementierung bestehender Marktverhältnisse befürchtet. Entwickler könnten mit einem Softwarepatent nicht nur die Verbreitung und Benutzung einzelner Softwareprodukte, sondern für sehr lange Zeitspannen (bis zu 20 Jahre), die im Computerzeitalter vielleicht nicht mehr angemessen sind, ganze Ideen und Verfahrensklassen reglementieren. Die Frage hinter der Debatte lautet: Wem wollen wir wofür und wie lange Monopolschutz gewähren?

Hypertext und Wiki

Soziologen wie Pierre Bourdieu haben wiederholt auf den Zusammenhang zwischen Kapitalakkumulation (Anhäufung von materiellen Gütern, aber auch von Wissen und Sozialkapital) und Benennungsmacht, der Autorität, auch in anderen gesellschaftlichen Feldern Einfluss auszuüben, hingewiesen.[11] Die Auflösung der klassischen Rollenverteilung zwischen Kommunikator und Rezipient durch neue Technologien ist vor diesem Hintergrund ein besonders interessantes Phänomen.

Bereits Vannavar Bush deutete in seiner Vision vom *Memory Extender*, einem Gerät zur assoziativen Verknüpfung und Bewahrung von Informationen unterschiedlicher Natur, das Konzept des Hypertextes an.[12] Ted Nelson griff dieses in den siebziger Jahren auf und verband es explizit mit sozialen Forderungen nach mehr Freiheit und Gleichheit.[13] Personen, denen viele Informationen bisher nur in der passiven Position des Rezipienten verfügbar waren, sollten durch vernetzte Computersysteme in die Lage versetzt werden, auch als Kommunikatoren an Informationsaustauschprozessen teilnehmen zu können. Was ursprünglich mit individueller Website-Gestaltung von Privatleuten begann, findet mit Weblogs (Internettagebüchern), Podcasts (privaten Audio-Dateien) und Video-Podcasts einen vorläufigen Höhepunkt. Ehemals passive Rezipienten können sich zu aktiven Sendern aufschwingen und ihre eigenen Radio- oder Fernsehshows anbieten. Podcasting entwickelte sich seit August 2004 zu einem sozialen Phänomen mit vielen Millionen Zuhörern und mehreren zehntausend aktiven Podcastern.

Eine „vielseitige, aktive und gestaltende Beteiligung am politischen Geschehen und damit eine größere Einflussnahme auf die politische Willensbildung“ durch die Bürgerinnen und Bürger verspricht sich auch die Enquete-Kommission des Bundestages „Zukunft der Medien in Wirtschaft und Gesellschaft“ von den Neuen Medien.[14] Die FDP versuchte im Bundestagswahlkampf 2005 mit der Initiative www.deutschlandprogramm.de, die Partizipation mit Hilfe des Internets zu erweitern: In moderierten Foren hatten Interessierte die Möglichkeit, an der Erstellung des Wahlprogramms mitzuwirken.

Der Erfolg des World Wide Web (WWW) seit Anfang der neunziger Jahre ist nicht zuletzt auf die Umsetzung des Hypertextkonzepts zurückzuführen, wie die Begriffe Hypertext Transfer Protocol (HTTP) oder Hypertext Markup Language (HTML) zeigen. Streng genommen wurde im WWW über viele Jahre hinweg nur ein Aspekt des von Nelson anvisierten Hypertext-Konzepts realisiert: die nicht-lineare Informationsdarbietung. Hypertexte in Form von Websites waren weiterhin von Kommunikatoren verfasst. Zwar erleichterte es die einfach erlernbare HTML-Sprache, sich aus der passiven Rolle des Rezipienten in die profilierte Position des Kommunikators zu versetzen. Man blieb aber weiterhin entweder Kommunikator oder Rezipient.

Das Phänomen, dass diese Rollen gezielt aufgelöst werden, findet sich erst in neueren Angeboten, etwa bei den so genannten Wikis: „Bei Wikis handelt es sich um im Internet verfügbare Seitensammlungen, die nicht nur von jedem Nutzer gelesen, sondern auch ge-

[11] Vgl. Pierre Bourdieu, Sozialer Raum und Klassen. Leçon sur la leçon. Zwei Vorlesungen, Frankfurt/M. 1985.

[12] Vgl. Vannevar Bush, As we may think, in: Atlantic Monthly, 176 (1945), S 101–108.

[13] Vgl. Theodor-Holm Nelson, Literary Machines, (Eigenverlag) 1981, S. 0/2 ff. und 2/61.

[14] Deutscher Bundestag, Schlussbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft“. Deutschlands Weg in die Informationsgesellschaft, Drucksache 13/1104, Bonn 1998, S. 79.

ändert und gelöscht werden können. Sie sind somit offene Content-Management-Systeme, die ohne vorherige Anmeldung und Authentifizierung auf jede Art der Kontrolle verzichten. Trotz dieses zunächst chaotisch und unkontrolliert anmutenden Konzepts verbirgt sich dahinter ein äußerst erfolgreicher Ansatz eines kollaborativen Wissensmanagements, das Schreiben wird als offener, kollektiver Prozess verstanden. Die gleichberechtigte Gestaltungsfreiheit jedes einzelnen Nutzers macht es zu einem demokratischen und partizipativen Ansatz der Wissensgenerierung."[15]

Ein besonders erfolgreiches Projekt dieser auf freies Teilen von Information ausgerichteten sozialen Bewegung ist Wikipedia, eine freie Enzyklopädie, zu der jeder sein Wissen beisteuern kann. 2001 startete die von der Non-Profit-Organisation Wikimedia betriebene Enzyklopädie in englischer Sprache. Mittlerweile enthält Wikipedia hunderttausende Artikel in über hundert Sprachen. Für die Nachhaltigkeitsdebatte sind Projekte wie Wikipedia trotz aller Negativschlagzeilen der jüngsten Vergangenheit hinsichtlich der Zuverlässigkeit „sozialer Software"[16] deshalb bedeutsam, weil sie die soziale Forderung nach mehr Gleichheit im Informationsaustausch und die Unabhängigkeit von Benennungsmacht und ökonomischem Kapital umsetzen.

Die Leichtigkeit, mit der man im WWW als Kommunikator aktiv werden kann, ist gelegentlich auch kritisiert worden. Joseph Weizenbaum etwa verglich das Internet mit einem Schrottplatz, in dem durchaus die eine oder andere Perle zu finden sei, die jedoch müsse man lange suchen.[17] Er kritisiert vor allem, dass die zentrale Stellung im Internet und somit die wahrgenommene Wichtigkeit einer Information nicht länger vom Wissen oder der Fachkompetenz ihres Verfassers, sondern vornehmlich von ihrem Google-Ranking abhängig sei. Auf diese Weise, so seine Sorge, würden sich langfristig nicht die besten Informationen, sondern die am schnellsten erreichbaren durchsetzen.

Ausblick

Nachhaltigkeitsdebatten im Sinne von Aushandlungsprozessen zwischen ökonomischen, sozialen und ökologischen Interessen finden sich innerhalb der IT-Welt zuhauf, auch wenn sie selten explizit mit dem Begriff Nachhaltigkeit assoziiert werden. Manche dieser Debatten existieren bereits seit Jahrzehnten, andere sind noch jung. Einige vermögen weltweit die Gemüter zu erhitzen, andere sind von lokal begrenztem Interesse. Die Liste ließe sich mit Schlagworten wie Datenschutz, Bildschirmarbeitsverordnung, *Social Software*, E-Government oder Software-Piraterie beliebig erweitern.

Sicherlich wird man den Debatten nicht immer vollständig gerecht, wenn man sie auf ihren normativen Grundgedanken, nämlich den Ausgleich zwischen ökonomischen, sozialen und ökologischen Interessen reduziert. Der Vorteil einer solchen Reduktion besteht allerdings darin, diese Debatten für Außenstehende zu öffnen und ihnen zu vermitteln, worum es geht und ob sie selbst betroffen sind. Dies ist die Grundlage für die Partizipation möglichst breiter Bevölkerungsschichten an der Beantwortung der Frage: „In welcher Welt wollen wir mit welcher Technik leben?" Eine solche Partizipation wiederum ist eine notwendige Voraussetzung für das, was die Bundesregierung als Nachhaltigkeit definiert: ein gesellschaftlicher Zustand, der in einem diskursiven Verfahren als wünschenswert und gerecht ermittelt wurde.[18]

Internet-Empfehlungen des Autors
www.itu.int/wsis/
www.computertakeback.com/
www.fsf.org/
http://de.wikipedia.org/wiki/Wikipedia
www.empa.ch/sis

[15] Matthias Barth, Internetbasierte Nachhaltigkeitskommunikation, in: Gerd Michelsen/Jasmin Godemann (Hrsg.), Handbuch Nachhaltigkeitskommunikation, München 2005, S. 270.
[16] Vgl. z. B. Bernd Graff, Unleserlicher Mist. Die Online-Enzyklopädie Wikipedia ist entzaubert, in: Süddeutsche Zeitung vom 7. 12. 2005.
[17] Vgl. Joseph Weizenbaum, Computermacht und Gesellschaft, Frankfurt/M. 2001, S. 15 ff.
[18] Vgl. Jörg Tremmel, Nachhaltigkeit als politische und analytische Kategorie, München 2003, S. 38.

Herausgegeben von
der Bundeszentrale
für politische Bildung
Adenauerallee 86
53113 Bonn.

Redaktion
Dr. Katharina Belwe
Dr. Hans-Georg Golz
(verantwortlich für diese Ausgabe)
Dr. Ludwig Watzal
Sabine Klingelhöfer
Andreas Kötzing (Volontär)
Telefon: (0 18 88) 5 15-0
oder (02 28) 36 91-0

Internet
www.bpb.de/publikationen/apuz
E-Mail: apuz@bpb.de

Druck
Frankfurter Societäts-
Druckerei GmbH,
60268 Frankfurt am Main

Vertrieb und Leserservice
Die Vertriebsabteilung der
Wochenzeitung Das **Parlament**
Frankenallee 71–81,
60327 Frankfurt am Main,
Telefon (0 69) 75 01-42 53,
Telefax (0 69) 75 01-45 02,
E-Mail: parlament@fsd.de,
nimmt entgegen:

- Nachforderungen der Zeitschrift Aus Politik und Zeitgeschichte
- Abonnementsbestellungen der Wochenzeitung einschließlich APuZ zum Preis von Euro 19,15 halbjährlich, Jahresvorzugspreis Euro 34,90 einschließlich Mehrwertsteuer; Kündigung drei Wochen vor Ablauf des Berechnungszeitraumes;
- Bestellungen von Sammelmappen für APuZ zum Preis von Euro 3,58 zuzüglich Verpackungskosten, Portokosten und Mehrwertsteuer.

ISSN 0479-611 X

APuZ

Nächste Ausgabe 7/2006 · 13. Februar 2006

Inszenierte Politik

Digitalisierung · Datenschutz

APuZ 5–6/2006