Datenschutz in einem informatisierten Alltag

Prof. Dr. Alexander Roßnagel

FRIEDRICH EBERT STIFTUNG

Gutachten
im Auftrag der Friedrich-Ebert-Stiftung

ISBN: 978-3-89892-681-2

Herausgeber: Stabsabteilung der Friedrich-Ebert-Stiftung
Redaktion: Beate Martin, Thomas Dreher

Hiroshimastraße 17, D–10785 Berlin
Stabsabteilung, www.fes.de/stabsabteilung

Umschlag: 2007, minus design, Berlin. www.minus.de
Foto: Johannes Beck
Gestaltung: Doreen Engel, Berlin
Druck: bub Bonner Universitäts-Buchdruckerei

Printed in Germany 2007

INHALT

THESEN

1. Allgegenwärtige Datenverarbeitung (Ubiquitous Computing) wird in den nächsten Jahren in kleinen Schritten Realität – nicht weil der Staat dies anordnet oder große Unternehmen dies erzwingen, sondern überwiegend weil die Nutzer dies wollen. Sie versprechen sich davon die Erfüllung ihrer Träume, ihre Sinne zu erweitern, ihr Gedächtnis zu unterstützen, sich von Arbeit zu entlasten und die eigene Sicherheit zu erhöhen.
2. Zunehmend werden die Gegenstände und Umgebungen des Alltags Sensoren und Prozessoren enthalten. Sie werden allgegenwärtig personenbezogene Daten automatisiert erheben und verarbeiten. Allgegenwärtige technische Unterstützung ist nur möglich durch Infrastrukturen zur allgegenwärtigen Kontrolle.
3. Einen Schutz zur freiheitsförderlichen Nutzung der Daten kann das geltende Datenschutzrecht nur bieten, wenn die künftigen Problemlagen seinem „Erwartungshorizont“ entsprechen. Dies wird nur dann der Fall sein, wenn nur wenige Instanzen mit klarer Rollenzuweisung beteiligt und die Verhältnisse überschaubar sind und die zu beurteilenden Handlungen nur Einzelfälle betreffen.
4. Im Rahmen allgegenwärtiger Datenverarbeitung wird das Datenschutzrecht aber zunehmend mit Situationen konfrontiert werden, in denen viele Beteiligte mit ständig wechselnden Rollen mitwirken, vielfältige Zwecke gleichzeitig verfolgt werden, Daten auch in privaten oder gemischt privat-geschäftlichen Kontexten verwendet werden, die Datenverarbeitung spontan von den Techniksystemen selbst organisiert wird, für

den Betroffenen unbemerkt erfolgt und in ihren Wirkungen undurchschaubar ist. Hierauf ist das Datenschutzrecht nicht eingestellt, weil seine Grundsätze der Transparenz, Zweckbindung, Erforderlichkeit, Kontrollfähigkeit und Mitwirkung des Betroffenen den Konzeptionen allgegenwärtiger Datenverarbeitung zur Profilbildung, zur Datenhaltung auf Vorrat und unbemerkten Datenverarbeitung im Hintergrund diametral widersprechen.

5. Das Datenschutzrecht wird die Entwicklung zur allgegenwärtigen Datenverarbeitung nicht aufhalten. Seine Aufgabe, informationelle Selbstbestimmung zu ermöglichen, wird es nur erfüllen können, wenn es sich den Bedingungen allgegenwärtiger Datenverarbeitung anpasst und dadurch Einfluss auf deren Entwicklung und Gestaltung gewinnt.
6. Notwendig ist daher eine Modernisierung des Datenschutzrechts, die Datenschutz in die Technik integriert und deshalb auch Anforderungen an Technikentwickler und -gestalter stellt, die Anreize schafft, Datenschutz von Anfang an zu berücksichtigen, die freiheitsförderliche Architekturen der Informations- und Kommunikationstechnik plant, die Vorsorge für die informationelle Selbstbestimmung trifft und eine systemische Grundrechtskontrolle institutionalisiert.

1. AUF DEM WEG ZUM INFORMATISIERTEN ALLTAG

Die Nutzung der Informations- und Kommunikationstechnik steht vor entscheidenden Veränderungen. In einigen Jahren wird nicht mehr der Computer als spezifisches Datenverarbeitungsgerät mit Tastatur und Maus für die Eingabe und einem Bildschirm für die Ausgabe im Mittelpunkt stehen. Vielmehr werden viele Alltagsdinge Daten verarbeiten können. Sie werden durch Sprache, Gestik, Mimik oder Berührung gesteuert oder erkennen aus den Umständen selbst, was von ihnen erwartet wird. Sie präsentieren die benötigten Informationen auf den Oberflächen von Wänden oder Gegenständen, in Brillen, Kleidung oder Kopfhörern. Vielfach führen sie die erforderlichen oder gewünschten Aktionen selbsttätig aus. Eine solche die Menschen alltäglich umgebende Informations- und Kommunikationstechnik wird im Amerikanischen Ubiquitous Computing, Pervasive Computing oder Ambient Intelligence genannt.[1] Im Deutschen könnte man sie allgegenwärtige Datenverarbeitung nennen.

Erste Schritte auf dem Weg in diese Welt wurden bereits gegangen: RFID-Chips auf Werkstücken, Werkzeugen, Produkten, Büchern, Ski-Pässen und Ausweispapieren, Lokalisierungsdienste und Navigationssysteme, Fahrerassistenzsysteme und autonome Arbeitsroboter. Weitere Anzeichen für die Fortentwicklung in diese Richtung sind auszumachen. In vielen Computer-Laboren wird an Bausteinen des Ubiquitous Computing gearbeitet. Den Blick auf das Zusammenspiel der vielen einzelnen Teile und das künftige Leben in einer Welt der allgegenwärtigen Datenverarbeitung bieten jedoch immer noch allein die Visionen, die mit dieser Entwicklung verbunden werden.

[1] S. zu minimalen, für das Thema dieser Untersuchung irrelevanten Differenzen Mattern 2005b, 40f.

Daher setzt die Untersuchung künftiger Auswirkungen eines informatisierten Alltags auf die informationelle Selbstbestimmung bei diesen Visionen an. Sie beschreiben im Guten wie im Schlechten mögliche Entwicklungen. Ubiquitous Computing wird eine besondere Durchsetzungskraft erhalten, weil sich viele versprechen, mit ihm lang gehegte Menschheitsträume verwirklichen zu können. Ubiquitous Computing wird in seinen Anwendungen und in seinen Auswirkungen wichtige Begrenzungen erfahren, weil viele die Verwirklichung von Alpträumen befürchten oder in Ansätzen erleben. Visionen, Träume und Alpträume gilt es daher als Einstieg in eine Vorstellungswelt des Ubiquitous Computing zu beschreiben (1.1).

Ob diese Entwicklungen möglich sind, hängt im ersten Schritt von den technischen Entwicklungsperspektiven und -potentialen ab. Daher sind anschließend die absehbaren technischen Entwicklungstrends, die den Weg zu einem Ubiquitous Computing ebnen könnten, zu beschreiben (1.2). Die technischen Möglichkeiten müssen, sollen sie realisiert werden, in künftigen Anwendungen der Informations- und Kommunikationstechnik genutzt werden. Welche Anwendungen auf dem Weg zu einem informatisierten Alltag erwartet werden können, wird dann im Folgenden dargestellt (1.3). Ob und wie diese in wirtschaftliche Technik- und Dienst-Angebote umgesetzt werden und von den Nutzern nachgefragt und genutzt werden, ist dann die nächste Hürde. Wie Lebensausschnitte aussehen könnten, wenn diese Hürden überwunden werden, wird dieses Kapitel abschließend in einigen Zukunftsbildern darstellen (1.4).

1.1 Visionen

Idee und Begriff des Ubiquitous Computing wurden erstmals von *Mark Weiser* formuliert. Bereits 1991 beschrieb er »ubiquitous computing« als eine »calm technology, when technology recedes into the background of our lives«. »It is invisible, everywhere computing, that does not live on a personal device of any sort, but is in the woodwork everywhere«.[2] In dieser Vision sind Computerfunktionen allgegenwärtig. Sie wirken unsichtbar und unterstützen den Menschen unaufdringlich bei seinen Tätigkeiten und befreien ihn weitestgehend von lästigen Routineaufgaben. »In the 21st century the technology revolution will move into the everyday, the small and the invisible.«

Für die Realisierung dieser Vision sind bereits viele Grundlagen gelegt: extrem miniaturisierte Sensoren, die vielfältige Umgebungsinformation erfassen, allerkleinste, energieeffiziente und preiswerte Prozessoren mit integrierter drahtloser Kommunikationsfähigkeit, Fernidentifikation von Dingen durch passive und praktisch unsichtbare Elektronik, präzise Lokalisierung von Gegenständen, flexible Displays auf Polymerbasis, elektronische Tinte und viele vergleichbare Entwicklungen. Prozessoren und Sensoren können aufgrund ihrer geringen Größe und ihres fast vernachlässigbaren Preises und Energiebedarfs leicht in andere Gegenstände integriert werden. Dadurch können Dinge Daten verarbeiten und kommunizieren. Durch Lokalisierungstechnologien können sie wissen, wo sie sich befinden, welche anderen Gegenstände oder Personen in der Nähe sind. Durch Datenspeicherung können sie sich erinnern, was in der Vergangenheit mit ihnen geschah. Aus ihrem Kontext können sie vielleicht sogar einfache Schlüsse über die Situation, in der sie sich befinden, ableiten. Wird die Umwelt mit Prozessoren und Sensoren ausgestattet, entstehen Sensornetze, die ihre Umgebung beobachten und Ereignisse melden. Die zukünftigen Rechner können als Schmuck oder als Teil der Kleidung den Menschen überall hin begleiten. Datenverarbeitungskapazität und Kommunikationsfähigkeit sind fast überall möglich. Damit werden die technischen Voraussetzungen für eine »totale Informatisierung« der Welt geschaffen.[3]

[2] Weiser, Scientific American 1991, 66 ff. Weiser war leitender Wissenschaftler am Computer Science Lab von Xerox Parc California.

[3] Mattern 2007a, 11.

Mit allgegenwärtiger Datenverarbeitung werden viele Hoffnungen verbunden. Weltweit wird geforscht und entwickelt, um eine Welt Wirklichkeit werden zulassen, in der die Datenverarbeitung zwar allgegenwärtig, aber in den Hintergrund getreten ist, den Menschen wie selbstverständlich umgibt und sich ihm und seinen Bedürfnissen anpasst.[4] Viele konzeptionelle Untersuchungen und szenarienhafte Darstellungen beschreiben die Zielsetzung dieser Forschung und Entwicklung als eine Zukunft, in der die Informationstechnik lang gehegte Menschheitsträume erfüllt. Beispielhaft können die Untersuchungen der Information Society Technologies Advisory Group (ISTAG),[5] aus dem Institut für Pervasive Computing der ETH Zürich,[6] Untersuchungen zur Umweltverträglichkeit von Ubiquitous Computing im Auftrag der TA Swiss,[7] Arbeiten im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI),[8] Szenarien und Untersuchungen des Ladenburger Kollegs »Living in a Smart Environment« der Karl Benz und Gottlieb Daimler-Stifung,[9] des Sonderforschungsbereichs 627 »Umgebungsmodelle für mobile kontextbezogene Systeme« (NEXUS) an der Universität Stuttgart,[10] der Rand Corporation,[11] der Humboldt-Universität in Berlin und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein[12] oder Diskussionen im Münchner Kreis[13] genannt werden.

4 S. Mattern 2003c, 4.
5 ISTAG 2001.
6 Bohn/Coroama 2002; Coroama, digma 2006, 106 ff.; Langheinrich 2001; Langheinrich 2005a; Langheinrich 2006; Langheinrich 2007a; Langheinrich 2007b; Mattern 2001; Mattern 2002; Mattern 2004; Mattern 2005a, Mattern 2007a; Mattern 2007b; Fleisch/Mattern 2005;
7 TA Swiss 2003.
8 BSI 2003; BSI 2004; BSI 2006.
9 Coroama u.a. 2003; Mattern 2003b; Mattern 2005c; Mattern 2007; Roßnagel 2004, 335 ff.; Müller, DuD 2004, 215 ff.; Müller/Handy, DuD 2005, 655 ff.
10 NEXUS 2005.
11 Rand Corporation 2005.
12 TAUCIS 2006.
13 Eberspächer/v. Reden 2006.

1.1.1 Träume

Allgegenwärtige Datenverarbeitung verspricht viele Sehnsüchte zu erfüllen, die viele Menschen schon immer – oft nur im Unterbewusstsein – hegen. Nun scheint die Informationstechnik diese Träume umsetzen zu können. Solange diese Hoffnung besteht, wird es für sehr viele verführerisch sein, sich auf die Erfüllung dieser Träume einzulassen.

Allgegenwärtige Datenverarbeitung verspricht zum einen, uns dem Traum eine *Erweiterung der Sinne* nahe zu bringen.[14] Vielfältigste Alltagsgegenstände nehmen über Sensoren, Mikrofone oder Minikameras Veränderungen in ihrer Umgebung wahr und bestimmen über Ortungsgeräte ihren jeweiligen Aufenthaltsort.[15] Diese Angaben können sie aufgrund eines Modells ihrer Umwelt einordnen und bewerten. Sie bieten dem Nutzer quasi »mitdenkend« kontextbezogen umfangreiche Zusatz- und Hintergrundinformationen an, die er allein durch seine eigenen Sinne nicht hätte wahrnehmen können. Beispielsweise erweitern Fahrerassistenzsysteme das Gesichtsfeld des Fahrers durch Abstandssensoren oder Funktechnik und können ihn so vor schwer oder nicht erkennbaren Hindernissen warnen. Künftige Verkehrstelematikdienste analysieren für den Fahrer die relevanten Verkehrsflüsse und bieten ihm eine dynamische Routenplanung, damit er ohne Staus und Hindernisse zu seinem Ziel gelangt. Sie beobachten für ihn die Umgebung der Fahrtroute und geben ihm je nach Situation und Ort hilfreiche Hinweise beispielsweise auf Sehenswürdigkeiten oder Restaurants. Informationstechnik im Kraftfahrzeug überwacht ständig den Zustand der relevanten Einzelteile und weist den Fahrer rechtzeitig auf Verschleiß und Reparaturnotwendigkeiten hin.[16]

14 Zum zentralen Motiv der Kompetenzerweiterung s. Hubig, in: NEXUS 2005, 7.
15 Mattern 2004, 320; Maurer, Informatik-Spektrum 2004, 45 ff.
16 S. z.B. Herrtwich 2003, 63 ff.; Herrtwich/Rehborn/Franz/Wex 2006, 132 ff.; BSI 2006, 27f., 83 ff.

Je nachdem, wo diese Sensoren angebracht sind, bieten sie ihrem Nutzer unterschiedliche Sinneserweiterungen. Sind sie in der Umwelt verteilt, ermöglichen sie ihm zeitgleich die Aufnahme von Eindrücken, obwohl er nicht am Ort des Geschehens ist. Sie ermüden nicht und sind nie unaufmerksam, sie bieten ihm eine permanente und umfassende Beobachtung. Beispielsweise ermöglichen sie ihm, den Zustand von Bauwerken und Maschinen oder ökologische Effekte wesentlich besser als bisher zu ermitteln und zu kontrollieren. Sind sie in der Kleidung angebracht, ermöglichen sie gesundheitlich relevante Parameter in unaufdringlicher Weise direkt am Körper zu messen. Dadurch kann jeder selbst diese Parameter wahrnehmen oder an einen Arzt oder Pfleger übermitteln. Für chronisch kranke oder ältere Personen kann dies bedeuten, dass sie länger ein selbst bestimmtes Leben führen können als bisher.

Die Kommunikation zwischen Mensch und Gegenstand erfolgt durch der Situation angepasste Eingabemedien wie Sprach-, Handschrift- und Bilderkennung sowie durch Ausgabemedien wie Sprache, Projektionen auf Wände oder leuchtfähiges Plastik. Smarte Brillen projizieren den Kommunikationsinhalt direkt auf die Netzhaut. Dadurch kann die körperliche Welt um zusätzliche Informationen angereichert werden. Ein anfahrender Bus teilt den an der Haltestelle Wartenden alle Stationen, an denen er hält, auf ihrem Endgerät mit. Das Fahrerassistenzsystem projiziert in unübersichtlichen Verkehrssituationen die zu fahrende Strecke auf die Windschutzscheibe.

Die virtuelle Modellierung der realen Welt erweitert die Vorstellungsräume. In diesen gemischten Welten kann zur Probe gehandelt werden, ohne tatsächliche Folgen oder gar Schäden zu verursachen. Dadurch kann der Nutzer Lerneffekte realisieren und seine Selbstkontrolle verbessern. In solchen risikoarmen Handlungsräumen können insgesamt gesehen Kompetenzen

entwickelt werden, wie dies in dieser Form bisher nicht möglich war.[17]

Ubiquitous Computing verspricht somit, die Sinne des Menschen zu erweitern und zu schärfen, dadurch seine Fähigkeit zu erhöhen, sich und seine Umgebung besser wahrzunehmen und zu überwachen.[18] Er hat seine Sinne nicht mehr nur in seinem Körper, sondern kann Ereignisse wahrnehmen, die weit von ihm entfernt stattfinden, und kann Entwicklungen und Zusammenhänge erkennen, für die es keine Sinnesorgane gibt. Durch die Analyse und Bewertung dieser Eindrücke fällt es ihm leichter, Situationen vorauszusehen und sich zielgerichteter und angepasster zu verhalten. Durch diese Wirkungen verspricht allgegenwärtige Datenverarbeitung, die Macht des Nutzers zu steigern.

Der Traum betrifft zum anderen die *Erweiterung des Gedächtnisses*. Die Dinge können ihre »Erfahrungen« protokollieren und dadurch ein eigenes »Gedächtnis« entwickeln. Diese Inhalte stehen dem Nutzer, dem Hersteller oder einem Diensteanbieter zur Verfügung.[19] Durch die Fähigkeit, sich selbst zu erklären, können etwa Produkte über Verfallsdatum, Gebrauchshinweise oder Unverträglichkeiten informieren. Das Auto und die Heizung können ihren Nutzer erkennen und sich von selbst auf ihn einstellen (Spiegel, Sitz, Temperatur, Luftfeuchtigkeit). Dinge können ihre Nutzer an Orte, Personen, Ereignisse oder Zustände kontextbezogen erinnern, etwa die Brille, die den Gesprächspartner erkennt, ihren Träger an ein bestimmtes Gesprächsthema.[20] Minikamera und Minimikrophon in der Brille können alles, was um den Nutzer herum geschieht, aufnehmen und so letztlich das gesamte Leben des Nutzers dokumentieren. Wenn er möchte, kann er sich dadurch an alles erinnern, was er je erlebt hat, und an alle Personen, denen er je begegnet ist.[21] Die Brille kann schließlich

17 Hubig 2007, 159. s. aber auch zum damit verbundenen Kompetenzverlust ebenda.
18 S. z.B. BMBF 2007, 22; Mattern 2005b, 46.
19 S. z.B. Mattern 2003c, 27; Roßnagel 2004, 341f.; Siemoneit, in: NEXUS 2005, 119.
20 S. z.B. Mattern 2004, 324f.; Maurer, Informatik-Spektrum 2004, 48.
21 S. z.B. Maurer, Informatik-Spektrum 2004, 45 ff.

einen elektronischen Assistenten losschicken, der in vernetzten Datenbanken nach nahezu beliebigen Informationen recherchieren kann, die sie dann für andere Beobachter unsichtbar, dem Nutzer darstellt. Muss dann noch jemand Fakten »auf Vorrat« lernen?[22]

In einem Beispiel *Weisers* fragt sich der Nutzer, wo er den schönen Anzug letzte Woche gesehen hat, den er längere Zeit betrachtet hat, wer diesen Anzug entworfen und ob der Laden noch weitere Exemplare dieses Anzugs hat. Sein Mobiltelefon und sein elektronischer Kalender erinnern sich, wo er längere Zeit in das Schaufenster eines Modegeschäfts geschaut hat. Ein Softwareagent findet die Marke und den Designer heraus und stellt fest, dass noch Exemplare des Anzugs vorrätig sind.[23]

Allgegenwärtige Datenverarbeitung verspricht somit eine Unterstützung des Gedächtnisses, indem sie dem Nutzer Zugriff auf individuelle und kollektive Datensammlungen und auf das »Gedächtnis« aller ihn umgebenden Dinge bietet. Trotz seines eigenen löchrigen Gedächtnisses ist es ihm möglich, sich an fast alles zu erinnern. Er kann entstandene Zweifel und Ungereimtheiten aufklären, Dokumentationen zu vielen erlebten Peinlichkeiten und beobachteten Untaten präsentieren oder gar dazu beitragen, Verbrechen aufzuklären.

Allgegenwärtige Datenverarbeitung verspricht drittens, den Traum einer *Befreiung und Erleichterung von Arbeit* wahr zu machen. Sie ermöglicht, Routineaufgaben und Alltagsentscheidungen auf technische Systeme zu delegieren.[24] Im Idealfall muss diese Delegation nicht immer neu vollzogen werden: Die Technik »verschwindet«, wird »selbstverständlich«, wird routinemäßig und damit unbewusst genutzt. Die Delegation kann zum einen

[22] Mattern 2007a, 26.

[23] Weiser, Scientific American 1991, 75.

[24] Hierin sieht auch die BSI-Studie 2006, 56, ein starkes Motiv zur Nutzung von Techniken des Ubiquitous Computing; nach Heesen, in: NEXUS 2005, 150, wird der Wunsch nach Komfort vor allem als Befreiung von Alltagshandlungen und als Arbeitsentlastung verstanden.

den Mitteleinsatz betreffen. Assistenzsysteme entlasten den Nutzer vom Einsatz der Mittel, erhöhen seine Effizienz, überwachen seinen Erfolg, veranlassen Nachsteuerungen und berichten über sein Gelingen.[25] Auf einer höheren Ebene kann eine Delegation auch dahingehend stattfinden, dass die Techniksysteme den Handlungsraum selbst in eine bestimmte Gestalt bringen, etwa indem sie den Mitteleinsatz strategisch bestimmen, selbst koordinieren und an die Verfügbarkeit von Ressourcen anpassen. Verändern sich die Problemlagen oder treten neue Umwelteffekte auf, können die Techniksysteme auch die Zwecksetzungen an die neue Situation anpassen.[26]

Die Befreiung von Arbeit durch Delegation an die Technik soll »Freizeit« ermöglichen. Wer auch in dieser Zeit erreichbar sein will, kann dies einem Stellvertreter übertragen. Softwareagenten, die ihre Umgebung wahrnehmen, können trotz Abwesenheit des Nutzers bestimmte Funktionsleistungen für das berufliche und soziale Netzwerk wahrnehmen. Sie managen die Erreichbarkeit des Nutzers und geben höfliche Auskünfte auf Kontaktwünsche.[27]

Ihr Nutzer muss sich um vieles nicht mehr selbst kümmern, wenn die Dinge in der Lage sind, sich gegenseitig zu identifizieren, sich ihre Zustände mitzuteilen, Umweltvorgänge zu erkennen und in einer vielfach sich selbst organisierenden Weise kontextbezogen zu reagieren. Beispielsweise kann die Haustechnik Licht, Klima und andere Funktionen selbst steuern, wenn sie über Sensoren erkennt, wer sich im Haus aufhält und welche Umgebungsbedingungen herrschen. Dinge, die sich identifizieren, können bei Ortsveränderungen beobachtet und gesteuert werden. Dadurch lassen sich viele Funktionen in Produktion und Logistik automatisieren. Dies entlastet nicht nur von Arbeit, sondern verspricht

[25] S. z.B. die Beispiele in Mattern 2003c, 21f.

[26] Hubig 2003, 211 ff.; Hubig 2007, 158.

[27] S. z.B. Heesen, in: NEXUS 2005, 195.

auch signifikante Kosteneinsparungen und erlaubt, Waren oder Dienstleistungen billiger anzubieten.[28]

Von allgegenwärtiger Datenverarbeitung dürfen die Nutzer – entsprechend dem Heinzelmännchenmotiv – eine allgegenwärtige Assistenz erwarten, die alles für sie erledigt.[29] Ihr Drang nach persönlicher Produktivität und Bequemlichkeit in einem immer komplexer werdenden Alltag dürfte eine wichtige Triebfeder für den Einsatz allgegenwärtiger Datenverarbeitung sein.

Allgegenwärtige Datenverarbeitung verspricht schließlich, den Traum von mehr *Sicherheit* zu erfüllen. Sie könnte es dem Nutzer erleichtern, über sein Lebensumfeld Kontrolle auszuüben und Ereignisse, Handlungen und Folgen selbstbestimmt und selbstverantwortlich aus- und herbeizuführen. Sie könnte es aber auch denjenigen, die für die innere und äußere Sicherheit einer Gesellschaft oder für die Sicherheit einzelner Anlagen oder Infrastrukturen verantwortlich sind, erheblich erleichtern, ihren jeweiligen Auftrag zu erfüllen.[30]

Allgegenwärtige Datenverarbeitung kann dem Nutzer helfen, sich sicherheitsfördernd zu verhalten. Beispielsweise verspricht die künftige Verkehrstelematik, die Sicherheit des Straßenverkehrs[31] durch Fahrerassistenzsysteme zu erhöhen, die dem Fahrer viele sicherheitsrelevante Entscheidungen abnehmen oder ihn durch Hinweise auf Hindernisse und Risiken unterstützen.[32] Ein anderes Beispiel sind medizinische Überwachungssysteme, die in die Kleidung integriert sind, Vitalparameter messen und den Nutzer

[28] S. z.B. Langheinrich 2007a, 61 mit mehreren Beispielen.

[29] S. Heesen, in: NEXUS 2005, 198

[30] Hierin sieht auch die BSI-Studie 2006, 56, vor allem für die Anwendungsbereiche Medizin, Autoverkehr und innere Sicherheit ein starkes Motiv zur Nutzung von Techniken des Ubiquitous Computing.

[31] Mit allgegenwärtiger Datenverarbeitung im Verkehr will die Europäische Kommission ihrem Ziel näher kommen, bis 2010 die Zahl der derzeit 41.000 Verkehrstoten in Europa zu halbieren. 93 Prozent der Unfälle sollen auf menschliches Versagen zurückzuführen sein – s. Frankfurter Rundschau vom 23.2.2006.

[32] BSI 2006, 89.

auf gesundheitsförderliches Verhalten hinweisen oder – bei kranken oder älteren Personen – die Daten zu einer medizinischen Überwachung weiterleiten.

Allgegenwärtige Datenverarbeitung kann den Nutzer gegen unerwünschte Ereignisse schützen. So wird etwa der Diebstahl eines Autos erheblich erschwert, wenn das Zündschloss erst genutzt werden kann, wenn es den Schlüssel eindeutig identifiziert oder den berechtigten Fahrer an seinem Fingerabdruck erkannt hat. Die Sicherheit gegen unerwünschte Eindringlinge kann durch Objektüberwachung, Zutrittskontrollen und Personenerkennung erhöht werden. Trittempfindliche Böden registrieren, ob sich in einem Raum Personen befinden und welchen Weg sie gehen, und lösen Alarm aus, wenn eine Bewegungsspur an einem Fenster oder einem Notausgang beginnt.[33]

Die allgemeine Sicherheit und Ordnung kann gestärkt werden, wenn allgegenwärtige Datenverarbeitung die Einhaltung von Sicherheitsregeln unterstützt oder erzwingt. So könnten zum Beispiel Verkehrszeichen, die mit Autos kommunizieren, die Einhaltung von Verkehrsregeln durchsetzen, etwa indem sie das Parken im absoluten Halteverbot unterbinden oder eine Überschreitung der Höchstgeschwindigkeit verhindern. Zigarettenautomaten machen die Ausgabe ihrer Ware vom Auslesen eines gültigen Ausweisdokuments abhängig, um Minderjährigen den Zugriff zu verweigern.[34]

Das Bewusstsein für die Verletzlichkeit einer offenen Zivilgesellschaft, die auf einen freien Informationsaustausch, Waren- und Personenverkehr beruht, ist in der Vergangenheit stetig gewachsen. In einer Welt der allgegenwärtigen Datenverarbeitung erscheint eine detaillierte Überwachung der zahllosen Güter- und Personenströme möglich. Dies verspricht, ohne zusätzlichen Aufwand mehr Sicherheit zu bieten, wenn die anfallenden Daten

[33] S. z.B. BSI 2006, 32.

[34] S. z.B. Langheinrich 2007a, 64.

ausgewertet werden, um Straftaten nicht nur aufzuklären, sondern vielfach auch bereits im Vorfeld zu verhindern.

Schließlich versprechen Techniken allgegenwärtiger Datenverarbeitung eine erhebliche Verstärkung militärischer Macht. Dies betrifft zum Beispiel die Ausrüstung des einzelnen Soldaten mit Systemen, die seine intellektuellen und sensorischen Fähigkeiten erweitern und unterstützen. Dies betrifft weiter die Überwachung sowohl größerer Gebiete als auch spezifischer Anlagen oder Stellen und die Identifikation einzelner Objekte oder Bewegungen. Dies gilt schließlich auch für den verbesserten Informationsaustausch zwischen der Streitkräfteführung, den einzelnen Einheiten und Soldaten, den Kampfmitteln und den Systemen zur Situationserkennung und -aufklärung. Die militärische Verwendungsmöglichkeit von Techniken allgegenwärtiger Datenverarbeitung hat stark zu ihrer Entwicklung beigetragen und wird auch künftig ein starker Antrieb für weitere Entwicklungen sein.

Der Einsatz allgegenwärtiger Datenverarbeitung zur Verstärkung der individuellen oder kollektiven Sicherheit ist vielfach eine explizite Zielsetzung, zumindest aber eine nicht unerwünschte Nebenfolge. Schließlich ist es ein Traum vieler Menschen, ihre Lebensumstände kontrollieren zu können und im Griff zu haben.

1.1.2 Alpträume

Allgegenwärtige Datenverarbeitung verspricht aber nicht nur Träume zu erfüllen, sondern ist auch der Stoff für Alpträume. Bereits *Mark Weiser* wies in seinem visionären Aufsatz darauf hin, dass Hunderte von Computern in jedem Raum, die Personen erfassen und mit leistungsfähigen Netzwerken verbunden sind, jedes bisherige totalitäre Regime wie die reinste Anarchie erscheinen lassen können. Die gesamte Datenverarbeitung, die unserer Bequemlichkeit dient, kann großen Schaden anrichten, wenn die Daten in die falschen Hände geraten. Nicht nur Vorgesetzte oder Handlanger, sondern auch übereifrige Beamte oder Marketingunternehmen können dieselben Daten, die die unsichtbaren Computer so komfortabel machen, zum Nachteil des Nutzers verwenden.[35]

Auf Potenziale und Risiken gesellschaftlicher Kontrolle und individueller Fremdsteuerung wurde nicht nur literarisch, sondern auch in wissenschaftlich fundierten Szenarien aufmerksam gemacht. Zum Beispiel entstand im Rahmen des EU-Projekts »Safeguards in a World of Ambient Intelligence« (SWAMI) ein Bericht über »Dark Scenarios on Ambient Intelligence: Highlighting Risks and Vulnerabilities«, in dem vier mögliche, aber nicht wünschenswerte Negativszenarien ausführlich diskutiert werden und dabei auf Gesichtspunkte wie Kontrollverlust, Probleme beim Angriff auf die Privatsphäre, Identitätsdiebstahl, falsche Verdächtigung aufgrund automatisierten Dataminings, Gefährdung der Unschuldsvermutung, detaillierte Profilbildung von Aktivitätsmustern mit der Gefahr der Diskriminierung sowie neuen Möglichkeiten von Verbrechen eingegangen wird.[36] Auf ethische Probleme künftiger Nutzungen der Informationstechnik weist die UNESCO hin.[37] Problematische Aspekte möglicher Zukunftsszenarien haben auch der DFG-Sonderforschungsbereich 627 »Umgebungsmodelle für mobile kontextbezogene Systeme« an der Universität Stuttgart[38] sowie das Forschungsprojekt »Technikfolgenabschätzung Ubiquitäres Computing und informationelle Selbstbestimmung« untersucht.[39]

Wird der Einzelne durch die Datenverarbeitung in seiner Umgebung und in den Alltagsgegenständen allgegenwärtig begleitet, wird sie unmerklich Teil seines Verhaltens und seines Handelns. Die Vielfalt der Datenverarbeitung führt zu einer exponentiellen Zunahme von personenbezogenen Daten mit hoher Aussagekraft.

---

35 Weiser, Scientific American 1991, 75.
36 S. SWAMI 2006a und 2006b.
37 UNESCO 2007.
38 NEXUS 2005.
39 TAUCIS 2006.

Sie erlauben individuelles Verhalten ebenso detailliert nachzuvollziehen wie kollektive Lebensstrukturen. Die Individualisierung der Unterstützung zwingt zu detaillierten Profilen mit Angaben zu Verhaltensweisen, Beziehungen, Einstellungen und Vorlieben.[40]

Allgegenwärtige Datenverarbeitung erfordert eine Infrastruktur zur permanenten Erhebung und situationsadäquaten Auswertung personenbezogener Daten, die zwangsläufig eine potenziell perfekte Überwachung ermöglicht.[41] Interessiert an diesen 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.[42] Dadurch kann die Ausübung von Grundrechten grundsätzlich gefährdet sein.[43]

Allein schon durch die umfassende Überwachungsmöglichkeit, die allgegenwärtige Datenverarbeitung bietet, könnte sich das politische und wirtschaftliche Machtgefüge verschieben. Neue, auf allgegenwärtige Datenverarbeitung zugeschnittene Geschäftsmodelle könnten eine stärkere Abhängigkeit von der zugrunde liegenden Technik und damit eine höhere Anfälligkeit im Krisenfall begründen. Nicht zuletzt besteht die Gefahr, dass wir das Vertrauen in eine kaum mehr durchschaubare, allzu smarte Umgebung verlieren und so grundlegend unsere Einstellung zu der uns umgebenden Welt ändern.[44] Während früher beträchtliche Energie aufgewendet werden musste, Daten zu erheben und zu verbreiten, wird es künftig umgekehrt sein. Es wird den Regelfall darstellen, dass ständig und überall Daten erhoben und verbreitet werden und es wird große Anstrengungen kosten, Daten zu vermeiden, lokal oder geheim zu halten. Einmal entstandene

40 S. hierzu näher unten 92 ff., 96 ff.

41 S. hierzu auch Langheinrich 2005, 336f.; Mattern 2003c, 31f.; Roßnagel 2005a, 53 ff.

42 S. Roßnagel/Müller, CR 2004, 628; zur Reduzierung der technischen Hemmschwelle für das private, gelegentliche Bespitzeln s. Mattern 2005a, 21.

43 SWAMI 2006a; Mattern 2007a, 25 ; Roßnagel/Müller, CR 2004, 628 ff.

44 Mattern 2007a, 26.

und verbreitete Daten wieder zu löschen, wird meist unmöglich sein.[45]

Die schöne neue Welt voller aufmerksamer und kommunikationsfreudiger Dinge kann leicht auch den Weg bereiten für einen Überwachungsstaat oder in einen von Konsumterror und ungebremstem Gewinnstreben geprägten Gesellschaft.[46] Daten werden bereits heute nicht nur von staatlichen Behörden ausgewertet, sondern in viel größerem Umfang von Privaten. Dies gilt aber nicht nur für Unternehmen, sondern potenziell auch für jeden Einzelnen. Mit Kleidungsstücken, die mit Sensoren, Minikameras, GPS-Lokalisatoren und Prozessoren ausgestattet sind, wird potenziell jeder zum ständigen Datensammler.[47] Neben oder an die Stelle des allwissenden »großen Bruders« treten zahllose »kleine Geschwister« in Form von neugierigen Nachbarn und eifersüchtigen Bekannten.[48]

1.1.3 Entwicklungsdynamik

Die Entwicklung zu einer allgegenwärtigen Datenverarbeitung wird schleichend und in kleinen Schritten erfolgen. Bereits heute sind bereits viele Vorboten der allgegenwärtigen Datenverarbeitung in Gebrauch. In den kommenden Jahren werden immer mehr einzelne Geräte mit Leistungsmerkmalen der Mobilität, der Ad-hoc-Vernetzung, der Kontextsensitivität und der Einbettung genutzt, soweit sie dem jeweiligen Nutzer einen spezifischen persönlichen Vorteil versprechen. Die so entstehenden anwendungs- oder herstellerabhängigen Insellösungen werden aber entsprechend ihrer Verbreitung nach und nach zu einer immer offeneren vernetzten Struktur allgegenwärtiger Datenverarbeitung zusammenwachsen.[49] Das, was daraus an Infrastrukturen

45 S. Mattern 2003c, 33; Roßnagel, Informatik-Spektrum 2005, 462f.

46 Mattern 2003c, 32.

47 S. z.B. Mattern 2005a, 21.

48 S. Roßnagel, Informatik-Spektrum 2002, 33 ff.

49 S. zu diesen zwei Entwicklungsstufen BSI 2006, 64f.

und Anwendungen entsteht, wird sich ungeplant einstellen. Für den jeweiligen Schritt wird es immer gute Gründe geben. Hinter seiner Umsetzung werden jeweils mächtige wirtschaftliche und politische Interessen stehen.

Die Nutzung allgegenwärtiger Datenverarbeitung wird in den seltensten Fällen erzwungen. Noch seltener dürfte ein Prestigeobjekt anstehen, das einen großen Entwicklungsschritt mit eindeutig negativen Folgen darstellt, so dass dagegen Widerstand entsteht und breit organisierbar ist. Selbst die Einführung der mit RFID und Biometrie versehenen Pässe im Oktober 2005 hat keinen solchen Widerstand provoziert. Noch weniger ist dies zu erwarten, wenn Anwendungen der allgegenwärtigen Datenverarbeitung eingeführt werden, um die Zahl der Unfälle zu senken und das Gesundheitssystem effizienter zu gestalten.[50] Auch wird es schwer sein, »gute« und »böse« Anwendungen zu unterscheiden. Vielfach sind die Folgen davon abhängig, wie die Technik genutzt wird, und sind nicht an der Technik als solcher festzumachen.

Allgegenwärtige Datenverarbeitung wird in den vielen kleinen Schritten ihrer Entstehung die Wünsche, Interessen und Träume der Menschen ansprechen. Diese werden die versprochenen Folgen haben wollen und viel Geld dafür ausgeben, ein »intelligentes« Haus, ein »intelligentes« Auto oder Kleider mit zusätzlichen Funktionen zu haben. Vermutlich werden die Vorteile allgegenwärtiger Datenverarbeitung so stark im Vordergrund stehen, dass es kaum zu kritischen Fragen kommt. Richtig eingeführt wird allgegenwärtige Datenverarbeitung den Menschen nicht als Einschränkung ihrer Freiheit, sondern als ein Garant dafür vorkommen. Für sie werden die Versprechen, die Träume zu erfüllen, näher liegen als die Furcht, dass sich die Alpträume verwirklichen. Wie bisher wird der bei Umfragen feststellbare typische Reflex, Überwachung zu befürchten, in der alltäglichen Praxis bei den Nutzern ausbleiben, wenn mit der Nutzung

[50] Ähnlich auch Langheinrich 2007a, 66.

eines kleinen Bausteins allgegenwärtiger Datenverarbeitung ein konkreter persönlicher Mehrwert zu erwarten ist: vereinfachte Abläufe, günstigere Preise und ein sichereres Leben.[51] Die Möglichkeit, ein praktisch lückenloses, weltweites Bewegungsprofil zu erstellen, hält kaum jemand davon ab, ein Mobiltelefon zu nutzen, ebenso wenig wie die Möglichkeit, ein Kauf- und Bewegungsmuster zu erstellen, von der Nutzung einer Kreditkarte abschreckt. Die erfahrbaren täglichen Vorteile überwiegen in der individuellen Bewertung die abstrakten, verborgenen Risiken.

Wenn Anwendungen der allgegenwärtigen Datenverarbeitung einen tatsächlichen Mehrwert für den Nutzer bieten, dürften die derzeit diskutierten negativen Folgen für viele kaum noch wahrzunehmen sein. So scheint es durchaus realistisch, dass sich viele Bausteine allgegenwärtiger Datenverarbeitung nach und nach durchsetzen werden.[52] Dieser Trend wird sich zunehmend verstärken. Je mehr sich an solche Technologien gewöhnt und ihre Vorteile erfahren haben, desto mehr wollen sie nicht mehr missen, sondern weiteren Nutzen aus weiteren Anwendungen ziehen.

Die Entwicklung zu allgegenwärtiger Datenverarbeitung wird nicht zu verhindern oder substanziell aufzuhalten sein. Selbst wenn sie jemand aufhalten wollte, er hätte hierfür keine Instrumente und wäre den vielen Interessen, die in diese Richtung drängen, hoffnungslos unterlegen. Wenn die Alpträume sich nicht verwirklichen sollen und die Entwicklung zu allgegenwärtiger Datenverarbeitung die Welt lebenswerter machen soll, muss das Ziel darin liegen, die Potenziale zur Verwirklichung der Träume von den Potenzialen zur Realisierung der Alpträume zu trennen. Dies könnte als Kompromiss auch in der öffentlichen Meinung mehrheitsfähig sein.

Freiheit, Entfaltung und Demokratie zu fördern und – auch gegen technische Sachzwänge – zu schützen, ist die Aufgabe von Staat

[51] Ähnlich Langheinrich 2007a, 65, für RFID.

[52] Langheinrich 2007a, 61.

und Recht.[53] Gegenwärtig erfüllen beide diese Aufgabe durch das Datenschutzrecht und dessen Vollzug. Inwieweit dieses auf die künftigen Herausforderungen einer allgegenwärtigen Datenverarbeitung eingestellt und in der Lage ist, das genannte Ziel zu erreichen, ist das Thema dieser Abhandlung. Bevor dieses jedoch unmittelbar aufgegriffen werden kann, ist zu klären, welche Entwicklungsschritte bereits unternommen wurden, was bereits auf den Weg gebracht worden und was künftig noch möglich ist. Danach ist zu untersuchen, wie die realistisch erscheinende Entwicklung beeinflusst werden kann. Erst dann kann geprüft werden, wie die künftigen Anwendungen so gestaltet werden können, dass der Schutz der Persönlichkeit gewährleistet und informationelle Selbstbestimmung ermöglicht wird.

1.2 Technische Entwicklungsperspektiven

Viele Visionen des Ubiquitous Computing könnten in nicht allzu ferner Zukunft wahr werden. Jedenfalls aus technischer Sicht sind Entwicklungen zu erwarten, die als Grundlagen für die Umsetzung dieser Visionen anzusehen sind. Einige Entwicklungstrends erscheinen stabil und für die allgegenwärtige Datenverarbeitung von besonderer Relevanz.

1.2.1 Fortschritte in der Mikroelektronik und Energieversorgung

Von grundlegender Bedeutung sind die absehbaren Fortschritte in der Mikroelektronik.[54] Sie werden zu einer weiteren Miniaturisierung aller technischen Komponenten wie Prozessoren, Sensoren, Aktoren, Mikrofone und Kameras sowie zu einer Vervielfachung der Rechenleistung führen. Noch immer gilt das 1965

[53] S. z.B. BVerfGE 49, 89 (125 ff.); 65, 1 (56); 112, 304 (316).

[54] S. z.B. BMBF 2007, 15; Bohn u.a. 2002, 5; BSI 2003, 53; BSI 2006, 38 ff.; Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 47 ff.; Langheinrich/Mattern 2002, 7; Mattern, Informatik-Spektrum 2001, 145; Mattern 2004, 317; Mattern 2007a, 5f.; Fabian/Hansen, in: TAUCIS 2006, 15.

von *Gordon Moore* aufgestellte »Gesetz«, nach dem sich die Zahl der auf einem Chip integrierbaren elektronischen Komponenten etwa alle 18 bis 24 Monate verdoppelt.[55] Oder anders ausgedrückt: Die Leistungsfähigkeit von Prozessoren (bei eher abnehmender Größe und Preis) wird etwa alle anderthalb Jahre verdoppelt. Fachleute rechnen damit, dass dieses »Gesetz« noch mehrere Prozessorgenerationen gilt. Prozessoren werden somit weiterhin leistungsfähiger, kleiner und billiger werden. Die gleiche Leistungssteigerung dürfte auch für Speicherkapazitäten und für Kommunikationsbandbreiten gelten.[56] Vielleicht gilt das Moore'sche »Gesetz« sogar noch wesentlich länger – Prognosen dazu sind aber schwierig, da dies auch von nicht-technischen Faktoren, wie beispielsweise den ökonomischen Randbedingungen, abhängt.[57]

Auf der Grundlage dieses »Entwicklungsgesetzes« wird prophezeit, dass künftig kleinste und drahtlos miteinander kommunizierende Prozessoren »quasi im Überfluss« vorhanden sein werden. Durch diese absehbare »Überschwemmung« der Welt durch Rechenleistung wird ein Paradigmenwechsel in der Computeranwendung bewirkt: Sehr kleine und billige Prozessoren, Speicherbausteine und Sensoren können in viele Alltagsgeräte eingebaut werden und diesen eine Datenverarbeitung ermöglichen, mit deren Hilfe sie ihr Verhalten an den jeweiligen Nutzer oder an die jeweilige Situation anpassen können.[58]

Entscheidend für die wichtigsten Bausteine des Ubiquitous Computing sind die Fortschritte in der Befriedigung des Energiebedarfs.[59] Die Notwendigkeit der Energieversorgung wird sogar als »technologischer Engpass« auf dem Weg zur allgegenwärtigen

[55] S. Moore, Electronics 1965, 114.

[56] Coroama u.a. 2003, 7.

[57] Mattern 2007a, 6; Mattern 2003c, 5 ff.; zur Möglichkeit, Transistoren aus Atomen und Molekülen zusammenzusetzen, BMBF 2007, 16.

[58] Mattern 2003c, 10.

[59] S. hierzu z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 65 ff.; BSI 2006, 40 ff.; Mattern 2003c, 14 ff.; Fabian/Hansen, in: TAUCIS 2006, 15f.

Datenverarbeitung gesehen.[60] Der erste Schritt, den Energiebedarf zu befriedigen, ist ihn zu verringern. In der Vergangenheit wurden in der Chip- und Elektronikentwicklung erhebliche Fortschritte hinsichtlich der Energieeffizienz erreicht.[61] Weitere Fortschritte sind auch in der nahen Zukunft zu erwarten. Der zweite Schritt ist, für die nicht netzgebundenen, mobilen Systeme eine autarke Energieversorgung zu sichern. Diese kann zum einen über kleine, hochleistungsfähige Batterien erreicht werden.[62] Zum anderen geht die Entwicklung dahin, ganz ohne Batterien auszukommen und die notwendige Energie aus der Umgebung zu gewinnen. Hierfür wird an Kleinstakkumulatoren, die elektrische Energie über Photovoltaik gewinnen, an Thermogeneratoren, die elektrische Spannung aus Temperaturunterschieden bei zwei verschiedenen Metallen erzeugen, an piezoelektrischen Generatoren, die mechanische in elektrische Energie umwandeln, und an anderen Energiewandlern gearbeitet.[63]

1.2.2 Fortschritte in der Kommunikationstechnik

Die Entwicklung der Mikroelektronik wird unterstützt durch einen qualitativen Sprung in der Verfügbarkeit von drahtlosen Kommunikationstechniken für Lang-, Mittel- und Kurzdistanzen.[64]

Für das Mobilfunknetz sowie für Wireless LAN wird derzeit durch Technologien wie »Ultra Wide Band« (UWB) und ZigBee erreicht, dass die Kommunikationsmodule noch weniger Energie benötigen, noch kleiner werden und dass noch mehr Daten noch schneller »durch die Luft« transportiert werden können.

60 BSI 2006, 42.

61 Mattern 2003c, 15f.; Mattern 2005b, 54; BSI 2006, 41.

62 S. z.B. BSI 2006, 41; Mattern 2003c, 14.

63 S. z.B. BSI 2006, 40f.; Mattern 2003c, 15; Mattern 2005b, 54.

64 Zu dieser Forderung s. Weiser, Scientific American 1991, 74; zur Umsetzung s. z.B. BMBF 2007, 18f.; Eckert/Bayarou/Rohr, Informatik-Spektrum 2004, 12 ff.; Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 49; Eckert 2003, 91; Mattern 2004, 317f.; Mattern 2005b, 48 ff.; BSI 2006, 44 ff.

In diesem Bereich dürften künftig weitere Leistungssteigerung erwartet werden.[65] Über drahtlose Ad-Hoc-Netze nach dem Peer-to-Peer-Prinzip kann die Datenübertragung einfacher, schneller und kostengünstiger erfolgen.[66]

Für Sensornetze, bei denen nur sehr geringe Datenraten erforderlich sind, können künftig extrem kleine und energiesparsame Funkgeräte zum Einsatz kommen. Werden Sender und Empfänger mit mehr »Intelligenz« ausgestattet, um sich an die jeweilige Situation anzupassen, kann das verfügbare Frequenzspektrum auch wesentlich ökonomischer genutzt werden als bisher, so dass insgesamt in viel größerem Umfang, aber mit weniger Energie als heute »gefunkt« werden kann.[67]

Ein Kommunikationsprinzip, das für die Kommunikation mit Geräten und Dingen besondere Bedeutung haben wird, ist die »Near Field Communication« (NFC). Für sie genügt es, wenn einer von zwei Partnern mit einer aktiven Einheit ausgestattet ist. Passive Einheiten verfügen über keine eigene Energiequelle, sondern werden von der aktiven Einheit (mit einer Batterie) während der Kommunikation gleichzeitig mit Energie versorgt. NFC funktioniert dadurch allerdings nur über Distanzen von Zentimetern. NFC ermöglicht jedoch ein neues Kommunikationsparadigma: Kommunikation durch physische Nähe. Aktive NFC-Einheiten sind klein genug, um beispielsweise in einem Mobiltelefon untergebracht zu werden; passive Einheiten sind noch wesentlich kleiner und vor allem sehr billig.[68]

65 Erwartet werden z.B. WLAN-Hotspots mit Datenraten von über 1 Gbit/s – s. näher z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 53 ff.; Eckert/Bayarou/Rohr, Informatik-Spektrum 2004, 15 ff.; Mattern 2007a, 6; Fabian/Hansen, in: TAUCIS 2006, 28 ff.

66 S. z.B. Lindemann/Waldhorst, Informatik-Spektrum 2006, 222 ff.; Steinmetz/Wehrle, Informatik-Spektrum 2004, 51 ff.; Stieler, c't 2004/16, 79 ff.; Eckert/Bayarou/Rohr, Informatik-Spektrum 2004, 18 ff.

67 Mattern 2007a, 8; Stieler, c't 2004/16, 79 ff.; Sietmann, c't 2004/16, 87f.

68 S. z.B. Mattern 2005b, 49f., Mattern 2007a, 8; zu Wireless Personal Area Networks nach Standards wie Bluetooth oder IrDA s. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 55 ff.

Aus Nutzersicht kann es dabei so aussehen, als ob sich zwei benachbarte Geräte erkennen und miteinander kommunizieren, sobald sie sich berühren oder zumindest sehr nahe kommen. Indem beispielsweise ein NFC-fähiges Mobiltelefon an ein Objekt gehalten wird, das einen RFID-Chip enthält, kann dieser ausgelesen werden. Das Handy kann die gelesenen Daten dann entweder direkt interpretieren und anzeigen oder ergänzende Information über das Mobilfunknetz besorgen oder sogar mit einem zugehörigen Server im Internet interagieren, dessen Internetadresse auf dem RFID-Chip gespeichert ist.[69] So könnte man etwa zu Fahrplänen zusätzliche Informationen über die Züge erhalten oder zu Werbeplakaten zusätzlich Informationen über die beworbenen Produkte.

Im Rahmen von »Body Area Networks« kann künftig sogar der menschliche Körper selbst als Medium zur Übertragung von Signalen extrem geringer Stromstärken genutzt werden. Allein durch Anfassen eines Geräts oder Gegenstands kann es zur Übertragung von Daten kommen – etwa zur Übermittlung von Identifikationsdaten für die Überprüfung von Zugangsberechtigungen, die Personalisierung von Geräten oder die Abrechnung von Dienstleistungen.[70]

1.2.3 Fortschritte in der automatischen Identifizierung

Künftige Rechner sollten in der Lage sein, zu erkennen, welche Personen sie bedienen oder mit welchen Gegenständen sie in einem Raum zusammen sind. Dann können sie sich auf diese einstellen und gezielt Informationen erzeugen, herausgeben oder verweigern.[71] Für die Identifikation von Gegenständen und Personen sowie für die Kommunikation mit ihnen kann das Prinzip der Radio Frequency Identification (RFID) zur Anwendung kommen.[72] Es arbeitet – wie beim NFC-Prinzip – in der Regel mit aktiven und passiven Einheiten.

An den Gegenständen werden bis zu staubkornkleine Transponder (RFID-Tags) angebracht, in denen – je nach Prozessor – von wenigen bis zu einigen hundert Kbyte gespeichert werden können.[73] In ihnen können eine weltweit einmalige Kennung und eventuell weitere Daten gespeichert werden. Die Mikrochips können entweder nur ausgelesen oder auch beschrieben werden.[74] Die Tags verfügen in der Regel über keine eigene Energiequelle, sondern werden vom Lesegerät während des Auslesens gleichzeitig auch mit Energie versorgt.[75] RFID-Tags gibt es mit fallender Tendenz schon unter 10 Cent pro Stück.[76]

Das Lesegerät stellt die (drahtlose) Schnittstelle zu den RFID-Tags dar und verfügt typischerweise über einen separaten Mikroprozessor mit internem Speicher. Es kann den Inhalt des Tags auslesen oder dem Tag einfache (Schreib-)Befehle übermitteln.[77] Es kann in tragbaren Geräten wie einem Mobiltelefon oder einem PDA oder in stationären Geräten wie einem Türrahmen oder einem Terminal integriert sein.

Die Kommunikation zwischen Tag und Lesegerät erfolgt kontaktlos. Je nach verwendeter Frequenz und Energieverbrauch eines RFID-Systems kann die Reichweite der Kommunikations-

69 S. z.B. Mattern 2003c, 26 ff.; Mattern 2007a, 8.

70 Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 57; Mattern 2004, 318; Mattern 2007a, 8; Mattern 2003c, 13.

71 Weiser, Scientific American 1991, 69.

72 Finkenzeller 2002; Lampe/Flörkemeier 2005, 69 ff.; acatech 2006, 8; BSI 2004, 27 ff.; AK Technik 2006, 5f.; Mattern 2003c, 11 ff.; Mattern 2007a, 6 ff.; Langheinrich 2007a, 127 ff.; Behrendt/Erdmann/ Würtenberger, in: TA Swiss 2003, 61; Fabian/ Hansen, in: TAUCIS 2006, 26 ff.; FifF 2006; Kelter/Wittmann, DuD 2004, 331 ff.

73 S. Finkenzeller 2002, 23 ff.; AK Technik 2006, 5; zu unterschiedlichen RFID-Systemen s. BSI 2004, 38 ff.

74 S. näher BSI 2004, 30f.

75 S. z.B. Finkenzeller 2002, 22f.; BSI 2004, 31 ff. Aktive Tags mit einer eingebauter Batterie sind größer, schwerer und teurer.

76 Nach BMBF 2007, 21; Holznagel/Bonnekoh 2006, 9, wird 2008 mit einem Stückpreis von nur wenigen Cent gerechnet.

77 Lampe/Flörkemeier 2005, 70; Langheinrich 2007a, 127f.

verbindung wenige Zentimeter bis wenige Meter betragen.[78] Anti-Kollisions-Protokolle sollen verhindern, dass sich die mehr oder weniger zeitgleichen Antworten mehrerer RFID-Tags überlappen und dadurch gegenseitig stören. Sie ermöglichen, die vorhandenen RFID-Tags durch wiederholtes »Befragen« nach und nach zu identifizieren.[79]

Gegenüber dem optischen Auslesen eines Barcodes bietet die Verwendung von RFID-Tags signifikante Vorteile:[80] Sie ermöglichen erstens die genaue Identifizierung des Gegenstands, nicht mehr nur – wie bei Barcodes – einer Produktklasse. Sie ermöglichen zweitens, mehr Informationen auf dem Tag selbst unterzubringen oder durch Verknüpfung mit einer Datenbank spezifische Zusatzinformationen zu diesem Gegenstand abzurufen. Sie benötigen drittens keine Sichtverbindung zum Lesegerät, die bei Barcodes manuell hergestellt werden muss, sondern können prinzipiell ohne besondere Ausrichtung, das heißt auch »um die Ecke« oder »von hinten«, gelesen werden. Dies erleichtert eine automatisierte Identifizierung. Viertens können RFID-Tags beinahe beliebig in ein Produkt integriert werden. Sie können verborgen bleiben, sind besser gegen Schmutz oder Abnutzung geschützt und stören nicht das Produktdesign. Schließlich können sie fünftens prinzipiell durch kryptographische Protokolle gegen unerlaubtes Auslesen oder Duplizieren geschützt werden.[81]

Eine weitere Möglichkeit der Objektidentifikation bietet ein »Trusted Platform Module (TPM)«.[82] Während RFID sich als Identifikationssystem für Gegenstände ohne elektronische Bauteile empfiehlt, bietet sich TPM für Geräte an, die über einen Mikroprozessor und ein Kommunikationssystem verfügen. Das TPM ist

[78] S. z.B. Finkenzeller 2002, 22; AK Technik 2006, 5; Lampe/Flörkemeier 2005, 73 ff., 78; BSI 2004, 39f.

[79] BSI 2004, 34 ff.; Langheinrich 2007a, 128f.; Lampe/Flörkemeier 2005, 76f.

[80] Langheinrich 2007a, 126 ff.; acatech 2006, 11; BSI 2006, 26; Mattern 2003c, 12; Winand/Frankfurt 2007, 79.

[81] S. hierzu Finkenzeller 2002, 25.

[82] Brandl, DuD, 2005, 537; Yamada/Kamioka, IEICE Transactions on Communication 3/2005, 850f.

ein zusätzlicher Chip, der ähnliche Funktionen wie eine Smartcard bietet, aber fest mit dem Mainboard des Elektronikgeräts verbunden ist. Derzeit haben weit über 60 Millionen[83] Personal Computer und Notebooks, mit stetig steigender Tendenz, einen TPM integriert. Das TPM dient als Sicherheitsanker zur Identifizierung des Geräts, mit dem er physisch verbunden ist. Mit seiner Hilfe lassen sich vielfältige kryptographische Funktionen realisieren wie zum Beispiel das Generieren von asymmetrischen und symmetrischen Schlüsseln mit Hilfe eines hardwarebasierten Zufallszahlengenerators, das Erzeugen von Hashwerten und Signaturen, die Bereitstellung eines hardwaregeschützten Speicherbereichs, die Bereitstellung eines vertrauenswürdigen Zeitgebers (Tick Counter), der für die Validierung und Festlegung von Gültigkeitsdaten bei Zertifikaten genutzt werden kann, oder die Ermittlung der Integrität der Software und Übermittlung einer Integritätsbestätigung.[84] Mit dem TPM können in sicherer Weise auch verschiedene Identitäten erzeugt werden, die alle auf dieses Gerät zurückgeführt werden können. Mit Hilfe des TPM können Daten so verschlüsselt werden, dass sie nur auf diesem Gerät wieder gelesen werden können.[85] Diese spezifischen Funktionen des TPM sind die Grundlage für die Spezifikationen für sicheres Computing der »Trusted Computing Group (TCG)«.[86]

1.2.4 Fortschritte in der Lokalisierung

Ein Computer oder Gegenstand, der weiß, wo er sich befindet, kann sein Verhalten an diesen Ort anpassen, ohne hierfür künstliche Intelligenz zu benötigen.[87] Zur Lokalisierung mobiler Objekte bestehen verschiedene technische Ansätze. Bei Gegenständen mit einer Mobilfunkeinrichtung kann festgestellt werden,

[83] Reiner, DuD 2006, 666.

[84] Stumpf/Sacher/Roßnagel/Eckert, DuD 2007, 357 ff.

[85] S. BSI 2006, 69.

[86] Trusted Computing Group 2006.

[87] Weiser, Scientific American, 1991, 68.

in welcher Funkzelle sich das Objekt befindet. Die Größe einer Funkzelle beträgt bei GSM in Städten wenige hundert Meter, im ländlichen Raum jedoch bis zu 35 km. Da die Signalstärke mit zunehmender Entfernung von Sender und Empfänger abnimmt, kann dieser Faktor ebenfalls berücksichtigt werden. Dadurch kann die Basisstation einer Funkzelle die Entfernung des Objekts mit einer Genauigkeit von etwa 500 m bestimmen. Befindet sich ein Objekt im Überlappungsbereich mehrerer Funkzellen, kann die Position durch Messung der Laufzeitunterschiede im Prinzip auf etwa 300 m genau ermittelt werden. Bei UMTS, das zurzeit eingeführt wird, ist in technischer Hinsicht sogar eine bis zu zehn Mal genauere Lokalisierung möglich.[88]

Eine aufwändigere, aber präzisere Methode besteht in der Laufzeitmessung von Funksignalen und daraus abgeleitet der Entfernungsbestimmung. Dieser Ansatz wird von satellitengestützten Systemen benutzt, wie dem »Global Positioning System« (GPS), das eine Genauigkeit von wenigen Metern erreicht. Eine Verbesserung der Präzision wird von dem künftigen europäischen Galileo-System erwartet. Eine Einschränkung stellt dabei allerdings die Tatsache dar, dass dies bisher nur bei »Sichtkontakt« zu den Satelliten, vor allem also im Freien, funktioniert.[89]

In Städten, in denen mittlerweile eine hohe Dichte von WLAN-Basisstationen vorhanden ist, kann eine Lokalisierung über die Erfassung durch eine oder mehrere solcher Stationen erfolgen. Sind die Ortskoordinaten der festen Stationen[90] bekannt, kann eine Lokalisierungsgenauigkeit von 20 bis 40 m erreicht werden – auch innerhalb von Gebäuden, wo GPS bisher versagt. Städtische Bereiche können damit schon zu fast hundert Prozent abgedeckt werden.[91]

88 S. z.B. Mattern 2005b, 51; Mattern 2007a, 10; BSI 2006, 47.

89 S. z.B. BSI 2006, 47; Fabian/Hansen, in: TAUCIS 2006, 30f.

90 Öffentliche Datenbanken enthalten bereits mehrere Millionen Netze mit eindeutiger Kennung und den Ortskoordinaten – s. Mattern 2007a, 10.

91 S. z.B. Mattern 2005b, 51; Mattern 2007a, 10.

Noch genauer kann die Lokalisierung in Gebäuden erfolgen, in denen eine satellitengestützte Ortung nicht funktioniert. Hier können Signalgeber wie zum Beispiel RFID-Tags, Baken und WLAN-Zugangsstationen, deren Ort bekannt ist, mit dem zu lokalisierenden Gerät kommunizieren und den Standort an das Gerät oder einen zentralen Rechner übermitteln.[92]

Noch sind die Teilnehmermodule für die Lokalisierung für viele Anwendungen zu groß, zu teuer, zu ungenau und zu energiehungrig. Für größere und wertvolle Dinge, wie beispielsweise Mietautos, rechnet sich ihr Einsatz jedoch schon heute. An verbesserten Möglichkeiten zur Positionsbestimmung mobiler Objekte wird intensiv gearbeitet. Neben einer Erhöhung der Genauigkeit besteht das Ziel vor allem in einer deutlichen Verkleinerung der Teilnehmermodule, einer Reduktion des Energiebedarfs und der Entwicklung von Techniken, die auch in geschlossenen Räumen funktionieren.[93] Bald werden Chips für die satellitenbasierte Positionsbestimmung für Mobiltelefone und ähnliche Geräte verfügbar sein, die wesentlich schwächere Signale verarbeiten können und deutlich weniger Energie benötigen. Künftig ist auch an eine Lokalisierung von Schlüsseln, Haustieren, Koffern, Postsendungen, Containern, Waffen, diebstahlsgefährdeten Objekten und umweltschädlichen Stoffen zu denken.[94]

Verfügen Gegenstände über miniaturisierte Lokalisierungstechniken, können für sie »Fahrtenschreiber« entwickelt werden, die immer wissen, wo sich der Gegenstand befindet. Werden diese Daten zusammen mit der momentanen Uhrzeit oder einem Zeitstempel abgespeichert, kann für jeden beliebigen Zeitpunkt die »Lebensspur« des Gegenstands rekonstruiert werden. Durch den Abgleich verschiedener solcher Lebensspuren kann der gemeinsame Kontext verschiedener Dinge ermittelt werden. Waren etwa zwei Koffer zur gleichen Zeit im gleichen Hotelzimmer, kann mit

92 S. BSI 2006, 47.

93 BSI 2006, 47.

94 Mattern 2007a, 10, 18.

einer gewissen Wahrscheinlichkeit auf ein bestimmtes Verhältnis ihrer damaligen Besitzer geschlossen werden.[95]

1.2.5 Fortschritte in der Sensortechnik

Entwicklungen der Mikrosystemtechnik und vermehrt auch der Nanotechnik ermöglichen kleinste Sensoren, die unterschiedlichste Eigenschaften der Umgebung wie Druck, Ton, Licht, Bild, Beschleunigung, Temperatur, Feuchtigkeit, Durchfluss, Gase, Stärke eines Magnetfeldes und Strahlung aufnehmen und die gemessenen Werte in elektronischer Form weitermelden.[96] Sensoren stellen gewissermaßen die »Sinnesorgane« von Dingen dar, mit denen diese ihre Umwelt wahrnehmen können.[97] Bei der Sensortechnik wurden in den letzten Jahren bedeutende Fortschritte erzielt. Sensorbausteine können bereits auf einer fingernagelgroßen Platine Fühler für Licht-, Druck-, Beschleunigungs-, Temperatur-, Ton- und Bildsignale vereinen oder Tonsignale in der Länge fast eines menschlichen Lebens aufzeichnen. Selbst kleinste datenverarbeitende und kommunikationsfähige Sensoren sind zu erwarten, die als »smarter Staub« jede Umweltbedingung »hautnah« registrieren können.[98] Die Nanotechnologie stellt sogar hochempfindliche Sensoren im submolekularen oder atomaren Bereich zur Verfügung.[99]

Sensorchips im (Teppich-)Boden, die untereinander über leitfähige Fasern Daten austauschen, können durch ihre Druckempfindlichkeit registrieren, ob sich in einem Raum Personen befinden und welchen Weg sie gehen. So kann beispielsweise ein Alarm ausgelöst werden, wenn eine Bewegungsspur an einem Fenster oder einem Notausgang beginnt. Darüber hinaus wird daran gearbeitet, Personen an dem Bewegungsmuster, das sie

95 S. z.B. Mattern 2003c, 14; Mattern 2005b, 52; Müller, DuD 2004, 216.
96 S. z.B. BSI 2006, 43; Mattern 2003c, 11.
97 BMBF 2007, 21; Mattern 2004, 320.
98 UNESCO 2007, 52; Mattern 2007a, 14.
99 BSI 2006, 43.

durch Gewicht, Schrittlänge, Fußstellung und Bewegungsablauf verursachen, zu identifizieren. Dies könnte eine unauffällige und belästigungsfreie biometrische Zugangskontrolle ermöglichen.[100]

1.2.6 Fortschritte in den Ein- und Ausgabemedien

In der Vision des Ubiquitous Computing haben die meisten Rechner keine spezifische Eingabe- oder Visualisierungskomponente mehr.[101] Sie sind Teil der Umgebung und interagieren mit dieser oder anderen Rechnern. Der Mensch ist nicht mehr oder nur teilweise in den Datenverarbeitungsprozess eingebunden. Die allgegenwärtige Rechnertechnik reagiert weitgehend implizit auf die Wünsche und Erwartungen der Menschen. Dennoch wird es auch zu dieser Technikinfrastruktur Möglichkeiten der Mensch-Maschine-Kommunikation geben.

Die Schnittstelle zwischen Mensch und Technik wird künftig nicht mehr auf Bildschirm, Maus und Tastatur beschränkt sein, sondern sich den Umgebungs- und Nutzungsbedingungen anpassen. Dies wird möglich sein, weil auf zusätzliche neue Eingabemedien, wie Sprach-, Handschriften- und Bilderkennung, Steuerung mittels Blick und Gestik sowie neue Ausgabemedien wie Netzhautprojektion, akustische Sprachinformationen, »leuchtendes Plastik« oder »smartes Papier« zurückgegriffen werden kann.[102]

Für die Eingabe von Befehlen können Sensoriksysteme verwendet werden, die für Behinderte entwickelt worden sind, aber auch zur alltäglichen Kommunikation mit Informatiksystemen genutzt werden können. Diese nutzen zum Beispiel Kopf- oder Augenbewegungen, den Luftzug beim Anpusten oder die Messung von Gehirnströmen, um Computer zu steuern. Zu erwarten

100 S. z.B. BSI 2006, 32; Langheinrich 2005, 339f.
101 S. Weiser, Scientific American 1991, 68.
102 S. z.B. Maurer, Informatik-Spektrum 2004, 45; BSI 2006, 53f.; BMBF 2007, 22; Mattern 2003c, 12f; Mattern 2004, 320; Mattern 2007a, 9; Fabian/Hansen, in: TAUCIS 2006, 17.

ist auch, dass Eingaben über ein Kehlkopfmikrophon im Halsband bei geschlossenem Mund erfolgen. Denkbar ist sogar, diese Steuerungsfunktionen direkt über Körperimplantate zu realisieren.[103]

Fortschritte in der Materialwissenschaft ermöglichen künftig Licht emittierende Polymere (»leuchtendes Plastik«), auf deren Grundlage Displays aus dünnen und hochflexiblen Plastikfolien hergestellt werden können.[104] Die Folien können auf unterschiedlichste Gegenstände aufgebracht werden und diese zur Wiedergabe von gespeicherten Inhalten befähigen. Es wird aber auch an »elektronischer Tinte« und »smartem Papier« gearbeitet. Realisiert wurden diese zum Beispiel dadurch, dass in weniger als ein Millimeter großen Kapseln weiße und schwarze, elektrisch unterschiedlich geladene Pigmente »schwimmen«. Diese »Tinte« wird auf eine sehr dünne Plastikfolie aufgetragen. Legt man an einer Stelle der Folie eine positive oder negative Spannung an, dann fließen entweder die weißen oder die schwarzen Farbpigmente an die Oberfläche und erzeugen an dieser Stelle einen kleinen Punkt. Auf diese Weise kann dynamisch etwas geschrieben und später wieder gelöscht werden. Künftig könnte es solche beschichteten Folien geben, die sich wie Papier anfühlen und verhalten. Dieses könnte dann ein ideales Ausgabemedium für elektronisch gespeicherte Inhalte darstellen, das flexibel genutzt und herumgetragen werden kann.[105]

Eine andere Möglichkeit der Darstellung kann die Verbesserung der Beamertechnologie bieten. Sind zum Beispiel Mobiltelefone, PDA, RFID-Leser oder Zeigestifte mit einem leistungsfähigen, aber energiearmen Laserbeamer versehen, können sie die Präsentation in beliebiger Größe an die Wand, auf den Tisch oder an

[103] S. BSI 2006, 54; BMBF 2007, 22; Maurer, Informatik-Spektrum 2004, 45 ff.

[104] Mattern 2007a, 9; Mattern 2003c, 12; Mattern 2005b, 45; BSI 2006, 53f.;

[105] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 58; Maurer, Informatik-Spektrum 2004, 45; Mattern 2007a, 9; Mattern 2003c, 12; Mattern 2005b, 45f.; BSI 2006, 54.

beliebige Stellen beamen und dadurch sichtbar machen.[106] Auf diese Weise können auch virtuelle Tatstaturen projiziert werden, auf denen Eingaben durchgeführt werden können.[107]

In der Erprobung befinden sich auch so genannte Retinaldisplays. Das sind Brillen, die im Gestell einen kleinen Laser eingebaut haben. Der Laser erzeugt ein Bild, das auf ein kleines Prisma im Brillenglas gelenkt wird. Von dort wird es in das Auge gespiegelt und auf die Retina projiziert. Das Bild entsteht also nicht auf einem »Schirm«, sondern wird Punkt für Punkt direkt ins Auge geschrieben.[108] Solche Brillen könnten Bildschirme ersetzen und dem Nutzer Inhalte anzeigen, ohne dass die Umgebung dies bemerkt. Eine andere Möglichkeit stellen halbtransparente Brillen dar, auf die spezifische Informationen eingeblendet werden, die die Sicht auf reale Objekte überlagern.[109]

1.2.7 Fortschritte in der Kontextverarbeitung

Die Fortschritte in den Aus- und Eingabemedien, in der Sensortechnik, in der Lokalisierung und Identifizierung können jedoch nur dann zu einer Erweiterung der Sinne und zu einer Entlastung von Aufgaben führen, wenn die zusätzlich gewonnenen Daten automatisiert ausgewertet, aufgearbeitet und dargestellt werden können oder zu selbsttätigen Aktionen der allgegenwärtigen Datenverarbeitung führen. Sie sind die Grundlage dafür, dass Aufgaben an Technik delegiert und situationsadäquat bearbeitet werden können. Dafür sind aber außerdem geeignete Mechanismen notwendig für die Delegation von Aufgaben, die Erkennung und Bewertung des Kontextes und die strategische Nutzung der vorhandenen Ressourcen zur Informationsaufbereitung und -darstellung oder zur Durchführung von Aktionen.

[106] S. z.B. Maurer, Informatik-Spektrum 2004, 45; Mattern 2005b, 56f.

[107] S. z.B. Maurer, Informatik-Spektrum 2004, 45, 47.

[108] S. z.B. Mattern 2003c, 12f.; Mattern 2004, 324; Mattern 2007a, 13; Maurer, Informatik-Spektrum 2004, 45; BSI 2006, 53.

[109] S. z.B. Simoneit, in: NEXUS 2005, 113f., 119.

Zum einen ist Software erforderlich, die geeignet ist, Aufgaben zu übernehmen und selbsttätig zu erfüllen. An der Technologie für Softwareagenten, die solche Aufgaben stationär oder mobil erledigen, wird derzeit intensiv gearbeitet und es werden in diesem Feld auch große Fortschritte erzielt.[110] Softwareagenten sind Programme, die in der Lage sind, eine Aufgabe relativ selbständig auszuführen, ohne auf Anordnungen des Nutzers angewiesen zu sein. Sie können ein Personenprofil des Nutzers oder vom Nutzer definierte Verhaltensregeln aufnehmen, von sich aus aktiv werden und sich autonom an erfasste veränderte Bedingungen anpassen.[111] Mobile Agenten haben zudem die Fähigkeit, sich von einer Computerplattform auf andere fortbewegen zu können.[112]

Um Entlastung von Arbeit und das Erleben freier Zeit einerseits zu erreichen und andererseits das Ideal ständiger Erreichbarkeit zu verfolgen, kann der Agent als Stellvertreter des Nutzers agieren und ihm ein differenziertes Erreichbarkeitsmanagement anbieten, das die sozialen Netzwerke in unterschiedliche Klassen einteilt. Auch hierfür muss er seine Umwelt wahrnehmen und einordnen. Personen von großer Vertrautheit erreichen den Nutzer persönlich. Andere wichtige Kommunikationspartner werden mit autorisierten Auskünften des Agenten versorgt. Sonstige Kontaktsuchende erhalten höfliche Vertröstungen auf einen späteren Zeitpunkt oder Auskünfte des Agenten zu Themen, in denen er sich auskennt.[113]

Zum anderen wird für ein situationsadäquates Interagieren der Gegenstände ein Erkennen und Einordnen des Kontextes benötigt, letztlich ein Verständnis unserer Welt.[114] Derzeit wird daran gearbeitet, durch Klassifikation des Gegenständlichen der realen Welt (also gleiches gleich zu benennen) Umweltvorgänge einzuordnen und in einem weiteren Schritt deren Kontextbedeutung interpretatorisch zu erfassen.[115] Am Ende steht ein mehr oder weniger detailliertes Umgebungsmodell, das erlaubt, die aufgenommenen Kontextparameter situationsadäquat zu interpretieren. Durch den Zusammenschluss lokaler Umgebungsmodelle entstehen globale Umgebungsmodelle. Umgebungsmodelle sollen stationäre Objekte wie auch mobile Objekte der realen Welt enthalten. Außerdem sollen sie durch virtuelle Objekte und Dienste angereichert werden können.[116]

[110] S. z.B. Gitter 2007, 45 ff.; Busch/Pinsdorf 2007, 9 ff.; Roßnagel/Schnellenbach-Held/Geibig/Paul 2007, 25 ff.

[111] S. z.B. Roßnagel/Schnellenbach-Held/Geibig/Paul 2007.

[112] S. z.B. Busch/Pinsdorf 2007, 9 ff.; Peters/Pinsdorf/Roth 2007, 21 ff.; Gitter 2007, 60 ff.

[113] S. z.B. Heesen, in: NEXUS 2005, 195.

[114] S. z.B. Fabian/Hansen, in: TAUCIS 2006, 21 ff.

1.2.8 Verbleibende Problembereiche

Die dargestellten Fortschritte lassen – rein technisch gesehen – noch viele Fragen offen, die gelöst werden müssen, bevor die hier angedeuteten Möglichkeiten realisiert werden können.[117] Dies betrifft zum einen einzelne Entwicklungsengpässe wie zum Beispiel ausreichende Energie insgesamt und für die jeweils einzelne Anwendung oder ausreichende Kapazitäten für die verschiedenen Bereiche der Telekommunikation. Dies gilt aber auch für übergreifende Fragestellungen wie die Erarbeitung fehlender Standards, die eine Kompatibilität und Vernetzung der Einzelsysteme erst erlauben,[118] und für die Infrastrukturen, die in unterschiedlicher Skalierung die Kooperation zwischen Gegenständen ermöglichen sollen. Noch viele offene Fragen ergeben sich auch hinsichtlich der Verfügbarkeit, Verlässlichkeit und Sicherheit der ubiquitären Anwendungen.[119] Noch fehlt es auch vielfach an geeigneten neuartigen Interaktionsformen zwischen Menschen und den sie umgebenden Rechenkapazitäten. Schließ-

[115] S. hierzu z.B. Rothermel 2007, 32 ff.; Rothermel/Bauer/Becker 2003, 134 ff.; Gupta u.a., Informatik-Spektrum 2004, 35 ff.; BSI 2006, 54; s. auch näher SFB 627 »Nexus«, Vision, http://www.nexus.uni-stuttgart.de/de/ueberblick/vision/index.html, und das Forschungsprojekt Ambient Agoras, www.ambient-agoras.org.

[116] Rothermel 2007, 32.

[117] S. hierzu z.B. Mattern 2003c, 17.

[118] S. z.B. Fabian, in: TAUCIS 2006, 67.

[119] S. hierzu insbesondere BSI 2006.

lich sind viele Fragen des Kontext- und Weltverständnisses von Softwaresystemen zu lösen, die erst eine sinnvolle Unterstützung des Menschen durch die umgebenden Informationssysteme ermöglichen.

Diese noch offenen Probleme stellen die Vision einer allgegenwärtigen Datenverarbeitung jedoch nicht grundsätzlich in Frage. Sie können in einzelnen Bereichen oder für bestimmte Anwendungen ihre Einführung erschweren und ihre Verbreitung behindern. Dies dürfte vor allem die Geschwindigkeit betreffen, mit der Ubiquitous Computing zu einer alltäglichen Erfahrung wird. An der Lösung dieser Probleme wird allerdings intensiv geforscht und gearbeitet. Daher wird allgegenwärtige Datenverarbeitung nicht nur eine Vision bleiben, sondern früher oder später, in starkem oder weniger starkem Maß gesellschaftliche Realität werden. Deshalb macht es trotz der beschriebenen Probleme Sinn, sich zu vergegenwärtigen, welche Anwendungsfelder für Ubiquitous Computing zu erwarten sind und welche Auswirkungen allgegenwärtige Datenverarbeitung auf Individuen und die Gesellschaft insgesamt haben kann.

1.3 Anwendungsfelder

Diese technischen Entwicklungen bewirken durch ihre Existenz noch nicht das, was allgegenwärtige Datenverarbeitung ausmacht. Sie sind Grundlagen des Ubiquitous Computing, müssen zu seiner Realisierung aber noch zu sinnvollen, nützlichen und wirtschaftlichen Anwendungen zusammengefügt werden. Denkbare Anwendungsfelder sollen im Folgenden beschrieben werden. Sie dürften vor allem durch folgende Merkmale charakterisiert sein:

In der Welt des Ubiquitous Computing begleiten die mit Rechenkapazität ausgestatteten Alltagsgegenstände die Menschen bei ihren Tätigkeiten und unterstützen sie scheinbar mitdenkend in einer sich selbst organisierenden Weise. So könnten etwa Funktionselemente von Gebäuden wie Hinweistafeln, Türschilder, Fenster, Beleuchtungsanlagen oder Aufzüge sowie Einrichtungen der urbanen Infrastruktur wie Verkehrszeichen, U-Bahn- und Bushaltestellen oder Ladengeschäfte sowie Alltagsgegenstände wie Kleidung, Einkaufswagen oder Mülltonnen die Fähigkeit haben, sich gegenseitig zu identifizieren («Ich bin eine juristische Fachbuchhandlung«), sich ihre Zustände mitzuteilen (»Hier ist ein freier Parkplatz«) und Umweltvorgänge zu erkennen (»Kunde nimmt Produkt X aus dem Warenregal«). Darüber hinaus werden sie kontextbezogen reagieren können (»Kunde nimmt ein Produkt X zur Begutachtung in die Hand«). Diese Gegenstände fungieren dann nicht mehr nur als Träger und Mittler von Informationen, sondern generieren Informationen selbst, die sie untereinander austauschen, und »entwickeln« ein eigenes »Gedächtnis«.[120]

Durch die sich selbstorganisierende Verbindung der Gegenstände, die Zusammenführung und Aggregierung der Daten entsteht ein viele Lebensbereiche durchwirkendes Netz, in dem Körperlichkeit und Virtualität zusammenwachsen. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Durch die Verknüpfung von Informationsverarbeitung, Kommunikation und der von Modellen der Welterklärung unterstützten Abbildung realer Dinge in der virtuellen Welt wird ein Paradigmenwechsel in der Informationsgesellschaft eingeläutet.

1.3.1 Kommunikationsfähige Gegenstände

Allgegenwärtige Datenverarbeitung entsteht dann, wenn die Kapazität, Daten aufzunehmen, zu verarbeiten und auszutauschen, nicht mehr nur in »Computern« vorhanden ist, sondern potenziell in jedem Gegenstand. Dieser soll seine eigene Situation wahrnehmen, die dabei gewonnenen Daten verarbeiten und mit anderen Gegenständen oder Menschen kommunizieren können.

[120] Fleisch/Dierkes 2003, 149; Mattern 2005a, 24.

Dies setzt kleine und billige Mikroprozessoren, kleine und billige drahtlose Kommunikationsmodule, kleine und billige Sensoren und geeignete Softwareprogramme voraus. Diese Grundbausteine werden künftig vorhanden sein.[121] Sie stellen jedoch recht unterschiedliche Anforderungen an den Herstellungsprozess. Daher ist eine Integration derzeit noch teuer, aber nicht unmöglich. Ziel ist ein einziger kleiner Chip, der Umgebungsparameter wahrnimmt, diese verarbeitet und gegebenenfalls weitermeldet.[122] Bei Bedarf können die so ausgestatteten Dinge auch vom Menschen angesprochen werden oder ihre Daten für den Menschen mit situationsadäquaten Ausgabemedien darstellen.[123]

Wo Daten gespeichert werden und wo Datenverarbeitung stattfindet, spielt für die damit verbundene Funktionalität grundsätzlich keine Rolle. Sie kann im Mikroprozessor des Gegenstands stattfinden, kann aber auch außerhalb erfolgen. Wenn sie intern erfolgt, ist der Gegenstand nicht darauf angewiesen, dass er ständige Kommunikationsverbindungen hat. In diesem Fall reicht oft ein relativ einfacher Prozessor. Denn es geht im Regelfall nicht darum, Dinge wirklich »vernunftbegabt« zu machen, vielmehr sollen sie sich situationsangepasst verhalten können, ohne tatsächlich »intelligent« zu sein.[124]

Vielfach ist ausreichend, dass der Gegenstand einen RFID-Chip trägt. Durch diesen kann er eindeutig identifiziert werden. Die ihm zugeordnete Datenspeicherung und Datenverarbeitung kann dann in einem Hintergrundsystem stattfinden. Jeder Gegenstand kann auch eine IP-Nummer und eine Internet-Seite haben, auf der alle gewünschten Daten gespeichert und abrufbar gehalten werden. Um sie abzurufen und weiter zu verwenden, reicht es aus, wenn die ID des Gegenstandes ausgelesen und eine Verbindung zu der dieser ID zugeordneten Web-Seite des Gegenstands hergestellt werden kann. Dadurch kann beliebigen Dingen ein

[121] S. oben 26f., 28f., 36f. und 39f.
[122] Mattern 2007a, 12.
[123] S. hierzu oben 37f.
[124] Mattern 2007a, 12.

spezifischer Datensatz zugeordnet werden und ein »Internet der Dinge« entstehen.[125] Damit dürfte auch das Internet einen drastischen Wandel erleben – nachdem mittlerweile so gut wie alle Computer der Welt daran angeschlossen sind, steht nun seine Verlängerung bis in die letzten Alltagsgegenstände hinein an.[126]

Die – über das Internet zugänglichen – Datenbankeinträge stellen in gewisser Weise das externe »Gedächtnis« des Gegenstands dar. Zu jedem physischen Objekt kann es ein informationelles Gegenstück als »Datenschatten« irgendwo im Internet geben, dessen Adresse am physischen Objekt anhaftet.[127]

Zur Kommunikation können die Gegenstände nach Bedarf unterschiedliche Kommunikationstechnologien nutzen, je nachdem, ob nur eine Kommunikation über kurze Strecken mit dem Lese- oder Empfangsgerät eines Menschen oder eines anderen Gegenstands erforderlich ist oder eine Übertragung über weitere Strecken, ob nur eine ID auszulesen ist oder größere Datenmengen zu übertragen sind.

Sensoren werden die für den Gegenstand relevanten Umgebungsbedingungen aufnehmen oder seinen Standort feststellen können. Unter Umständen ist es auch notwendig oder hilfreich, die anderen in der Nähe befindlichen kommunikationsfähigen Gegenstände zu registrieren. Sofern eine Kommunikation mit Menschen gewünscht wird, sind geeignete Schnittstellen für die geeigneten Ein- und Ausgabemedien notwendig.

Derart ausgestattete Gegenstände bieten viele Vorteile: Sie können sich gewisse Vorkommnisse merken – wenn sie mit einem Lokationssensor ausgestattet sind, zum Beispiel, wo sie schon überall waren. Sie können sich – bei geeigneter Programmierung – auch kontextbezogen verhalten. Ein Rasensprinkler würde zum Beispiel neben den Feuchtigkeitssensoren im Boden auch die Wettervorhersage im Internet konsultieren, bevor er sich ent-

[125] Fleisch/Mattern 2005; BMBF 2007, 20f.
[126] Mattern 2007, 8f.
[127] S. Mattern 2003c, 27.

scheidet, den Rasen zu wässern.[128] Aufgrund ihrer Kommunikationsfähigkeit können sie auch anderen ihre Daten anbieten. Zum Beispiel könnte ein Auto andere Autos auf der Gegenfahrbahn vor einem Stau warnen. Ein im Autoschlüssel integrierter RFID-Chip wird beim Betätigen der Zündung von einem integrierten Lesegerät ausgelesen und identifiziert im Rahmen eines Authentisierungsprotokolls den Schlüssel als ein Original und deaktiviert nur dann die Wegfahrsperre.[129] Eine Mülltonne könnte die Recyclingfähigkeit der in sie eingefüllten Gegenstände erkennen und bei ihrer Abholung darüber informieren. Ein Arzneischrank könnte die Verträglichkeit seiner Medikamente für seine Nutzer und deren Haltbarkeit erkennen und im begründeten Fall diese warnen. Eine Wohnungsheizung könnte mit persönlichen Gegenständen der Bewohner kooperieren, um zu erfahren, ob mit deren baldiger Rückkehr zu rechnen ist, damit sie rechtzeitig die präferierte Temperatur und Luftfeuchtigkeit herstellen kann.[130] Wenn Alltagsgegenstände über ein Internet der Dinge flexibel mit Daten angereichert werden können, eröffnet dies in Zukunft weit über den vordergründigen Zweck der automatisierten Lagerhaltung oder des kassenlosen Supermarktes hinausgehende Anwendungsmöglichkeiten.[131] Dies ist die Grundlage für eine Anreicherung der körperlichen Welt durch vielfältige virtuelle Wirklichkeiten.

1.3.2 Anreicherung der körperlichen Welt

Die Bausteine des Ubiquitous Computing können verwendet werden, um die körperliche Welt kontextbezogen durch zusätzliche virtuelle Informationen oder ganze Informationsräume anzureichern. Diese »Augmented Realities« sind das Gegenteil von virtueller Realität.[132] Das Ziel der virtuellen Realität ist es, die reale Welt in Form digital verarbeitbarer Modelle möglichst gut im Computer abzubilden, etwa um Simulationen durchzuführen. So kann etwa zur Verkaufsförderung simuliert werden, dass der potentielle Käufer ein ausgewähltes Bekleidungsstück in verschiedenen Kontexten trägt, damit er dadurch seine Wirkung ausprobieren kann. Ein anderes Beispiel bieten Modelle technischer Systeme, die probehalber mit anderen Modellen zusammengebaut werden können und dadurch ermöglichen, die Funktionalität des Gesamtsystems und die Einpassung in die Umgebung zu testen.[133] In diesen Fällen können Modell und reale Welt ohne Interdependenzen nebeneinander existieren. Dagegen zielt die Anreicherung der körperlichen Welt darauf, die reale Welt mit Hilfe von Informationsverarbeitung zu »veredeln«. Es geht darum, real existierende Objekte mit zusätzlichen Informationen zu verknüpfen und ihnen virtuelle Objekte hinzuzufügen. Dadurch wird eine Symbiose aus realer Welt und digitalen Informationsräumen erzeugt.[134]

Beispiele können zum einen aus der Metapher des virtuellen Klebezettels entwickelt werden:[135] Reale Objekte werden mit zusätzlichen Daten annotiert, die etwa über eine Verknüpfung auf einem RFID-Tag erreicht werden können. Der Anwender erhält so Zugriff auf virtuelle Objekte, die mit Objekten in der realen Welt verknüpft sind. Denkbar ist auch, dass virtuelle Objekte mit einem bestimmten Kontext gekoppelt sind, zum Beispiel mit dem Aufenthalt an einem Ort, mit dem Zusammentreffen mit einer bestimmten Person, mit dem Eintreten eines bestimmten Zustands der Umwelt oder eines technischen Systems oder einer Kombination aus alledem. Tritt dieser Kontext ein, wird der Benutzer darüber informiert oder es wird automatisch eine Aktion aus-

[128] Mattern 2007a, 17.
[129] AK Technik 2006, 18f.; Langheinrich 2007a, 127.
[130] S. zu diesen Beispielen auch Mattern 2007a, 17.
[131] Mattern 2007a, 7.
[132] S. Weiser, Scientific American 1991, 66.
[133] S. z.B. Roßnagel/Schroeder 1999.
[134] Rothermel 2007, 32; Siemoneit, in: NEXUS 2005, 119.
[135] S. hierzu z.B. die »Tabs« in der Vision Weisers, Scientific American 1991, 68.

geführt.[136] So können etwa ein Filmplakat um weitere Informationen zu diesem Film, ein Fertiggericht um Empfehlungen zur Zubereitung, ein Bild in einer Ausstellung um Angaben zum Maler, zur Entstehung und zum künstlerischen Kontext, oder eine Maschine um eine Gebrauchsanweisung bereichert werden.

Eine andere Metapher ist die virtuelle Litfaßsäule:[137] Eine virtuelle Litfaßsäule wird an einem bestimmten Ort aufgestellt und besitzt einen Sichtbarkeitsbereich. Sie bietet Datensätze innerhalb ihres Sichtbarkeitsbereichs in Form von Postern an. Die hierarchisch strukturierten Poster sind Webseiten, die so an einen Ort gebunden werden. Für Poster und Litfaßsäulen können Zeiträume angegeben werden, in denen sie gültig sind.[138] Dadurch ist eine geographische Adressierung von Nachrichten möglich. Elektronische Dokumente können mit einem bestimmten Raumpunkt so verbunden werden, dass jeder, der durch den Eingang zu einem Raum geht, eine an die Wand projizierte oder auf sein persönliches Endgerät übermittelte Nachricht zu sehen bekommt.[139]

Eine dritte Metapher zur Anreicherung der körperlichen Welt ist der virtuelle Agent. Dieser kann per Projektion oder qua Datenbrille in der realen Welt »gesehen« werden und als Führer, Begleiter oder Lehrer zusätzliche Informationen zu dem jeweils Gesehenen oder Anregungen für weitere Handlungspläne bieten.[140] Der Agent kann als einfacher Pfeil in einem Navigationssystem erscheinen, als Navigationshilfe auf die Windschutzscheibe projiziert werden oder als Avatar sich mit dem Blick des Nutzers auf einen Ausschnitt der Realität mischen. Aber auch ohne Agentenbild könnten Informationen mit einer hochgenauen Positionsbestimmung des Nutzers verbunden werden – wenn etwa dem Monteur mittels einer halbtransparenten Brille die aktuellen

[136] BMBF 2007, 22; Simoneit, in: NEXUS 2005, 113.
[137] S. hierzu z.B. die »Pads« in der Vision Weisers, Scientific American 1991, 69.
[138] Rothermel 2007, 37.
[139] S. z.B. Simoneit, in: NEXUS 2005, 113
[140] S. z.B. BMBF 2007, 22; André/Rist 2001.

Maschinendaten oder Schaltkreiszeichnungen eingeblendet werden, die die realen Objekte überlagern.[141]

Durch diese informationelle Anreicherung kann es so erscheinen, als sei der jeweilige Gegenstand mitdenkend und passe sich der Umgebung und der Situation an. Selbst wenn der Gegenstand eigentlich nur seine Produktkennung preisgeben kann und ansonsten keine weiteren Ressourcen zur Datenverarbeitung hat, kann dieser Eindruck entstehen. Dann können nämlich vielfältige Ressourcen ihm virtuell »zu Hilfe kommen« und zusätzliche Daten und Dienstleistungen anbieten. Dadurch sind etwa Szenarien möglich, in denen jemand mit einer Reklametafel oder einem Filmplakat interagiert und dabei Videoclips zugespielt bekommt, Kinokarten reserviert oder Musik herunter lädt und dies später mit der Telefonrechnung bezahlt.[142] Auf diese Weise kann eine gewisse technische »Intelligenz« der Gegenstände simuliert werden.

Allgemein ist zu erwarten, dass zunehmend hybride Produkte entstehen werden, die sich aus physischer Leistung (z.B. ein Medikament mit seinen biochemischen und medizinischen Wirkungen) und Informationsleistung (bei diesem Beispiel etwa aktuelle Hinweise zum Verlauf einer Grippeepidemie) zusammensetzen. Anfangs werden von den informationstechnischen Möglichkeiten sicherlich eher hochpreisige Geräte und Maschinen profitieren, die durch sensorgestützte Informationsverarbeitung und Kommunikationsfähigkeit einen deutlichen Mehrwert erhalten. Sind die Grundtechniken und zugehörigen Infrastrukturen eingeführt, könnten bald darauf auch viele andere und eher banale Gegenstände ganz selbstverständlich das Internet mit seinen vielfältigen Ressourcen für die Durchführung ihrer Aufgaben nutzen.[143]

[141] S. Simoneit, in: NEXUS 2005, 113f., 119.
[142] S. z.B. Mattern 2003c, 26 ff.; Mattern 2007a, 8.
[143] Mattern 2007a, 18; Rothermel 2007, 31.

Der digitale Mehrwert, der durch zusätzliche an das Produkt gebundene Informationen entsteht, dürfte ein wesentliches Unterscheidungsmerkmal zu physisch vergleichbaren Erzeugnissen der Konkurrenz werden. Gewinnung und Bindung der Kunden könnten künftig sogar vorwiegend über diese Mehrwertdienste zu den jeweiligen Produkten erfolgen.[144] Die hybriden Produkte werden Informationen über ihre Nutzung und mögliche »Aufrüstungen« geben und dabei durch subtile Empfehlungen auch über »befreundete« Produkte aufklären. Umgekehrt erhalten Customer-Relationship-Systeme durch die Kommunikation mit solchen und über solche Produkte mehr und mehr präzise Angaben über die Kunden und deren Produktnutzung. Dies wird ihnen ein kundengenaues One-to-One-Marketing mit kundenbezogenen Preisdifferenzierungen ermöglichen, bei dem jeder Kunde einen individuellen Preis erhalten könnte, der idealer Weise genau seiner situativen Zahlungsbereitschaft entspricht.[145]

Diese Techniken können auch zur informationellen Anreicherung des Wissens über Menschen genutzt werden. Wenn der Mensch über Ausweise, Kundenkarten, Berechtigungen und ähnliches identifiziert wird und die RFID-Chips auf seinen Gegenständen mit Umgebungssystemen kommunizieren, kann zum Beispiel festgestellt werden, wo er sich jeweils befindet. Dies kann nicht nur das Finden von Freunden, Arbeitskollegen, Hausmeistern oder Notfallverantwortlichen erleichtern,[146] sondern auch für weitere Dispositionen relevant sein. Enthält beispielsweise die Bordkarte eines Flugreisenden einen RFID-Chip, so kann bei Passieren geeignet instrumentierter Stellen automatisch festgestellt werden, in welchem Flughafenbereich sich dieser befindet. Ein säumiger Fluggast braucht dann nicht mehr überall per Lautsprecher ausgerufen zu werden. Außerdem kann die Fluglinie entscheiden, ob es sich lohnt, noch auf den Fluggast zu warten.[147]

144 S. z.B. Mattern 2003c, 24.

145 S. z.B. Skiera/Spann 2002, 270 ff.; Pfaff/Skiera 2002, 24 ff.; Mattern 2003c, 25; Mattern 2004, 327; Coroama u.a. 2003, 21, 25, 110.

146 S. z.B. Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 57 ff.

1.3.3 Sensornetze

Sensoren könnten mit Funktechnologie und Kommunikationssoftware ausgestattet werden, so dass sie sich drahtlos vernetzen können. Dadurch erhält man so genannte Sensornetze.[148] Anwendungsbeispiele für Sensornetze, die sich regelrecht aufdrängen, sind zum einen die militärische Nutzung und zum anderen die Beobachtung der Umwelt. Auch Infrastruktursysteme, Verkehrssysteme und Fabrikationsprozesse könnten von einem genauen und »unaufdringlichen« Monitoring profitieren.

Wird etwa eine große Zahl hochgradig miniaturisierter Funksensoren großflächig in die Umwelt eingebracht, indem sie im Extremfall zum Beispiel aus einem Flugzeug abgeworfen werden, können sie flächendeckend Überwachungsaufgaben wahrnehmen. Jeder einzelne Sensorknoten in einem solchen Verbund beobachtet zunächst seine unmittelbare Umgebung. Die Sensoren können sich aber mit benachbarten Sensoren ad hoc vernetzen, ihre Arbeit untereinander abstimmen und relevante Beobachtungen austauschen. Wird es bei einem Sensor zum Beispiel heiß, kurze Zeit später bei einem benachbarten Sensor und wieder etwas später bei einem dritten Sensor, so lässt sich daraus auf ein Feuer schließen und es kann mit weiteren geeigneten Daten der Umfang sowie die Ausbreitungsrichtung und -geschwindigkeit des Brands berechnet werden. [149]

Prototypen solcher Sensornetze existieren bereits, allerdings steht man hier erst am Anfang der Entwicklung. Sobald kleine und energieeffiziente Sensoren, die sich automatisch vernetzen,

147 S. zu diesem Beispiel Mattern 2005b, 56.

148 S. z.B. BSI 2006, 43; Mattern 2003c, 17 ff.; Mattern 2004, 325; Mattern 2005a, 13; Mattern 2007a, 14; BMBF 2007, 21.

149 Mattern 2007a, 14.

massenhaft hergestellt werden können, lassen sich mit ihnen vielfältige Phänomene der Welt in bisher nie erreichter Genauigkeit beobachten. Durch die geringe Größe der Sensoren und dadurch, dass sie keine physische Infrastruktur wie Verkabelung und Stromanschlüsse benötigen, kann die Instrumentierung in flexibler und nahezu unsichtbarer Weise geschehen, ohne die beobachteten Aspekte wesentlich zu beeinflussen.[150]

Mit Sensornetzen könnte die Erhebung von Daten revolutioniert werden. Während in der Vergangenheit die Daten durch Kommunikation oder durch visuellen Kontakt erhoben und manuell in Informationssysteme eingegeben werden mussten und sich deshalb auf wenige charakteristische Angaben zu einem bestimmten Zeitpunkt an einem bestimmten Ort beschränkten, können bei Sensornetzen alle diese Beschränkungen entfallen. Sie erfassen in einem bestimmbaren Gebiet über einen wählbaren Zeitraum viele relevante Angaben automatisch und stellen sie in Realzeit online zur Verfügung. Sie setzen dafür an den physischen Phänomenen selbst an, nicht an ihrer menschlichen Wahrnehmung oder an der Kommunikation über sie. Messen oder erfassen können Sensoren akustische und visuelle Phänomene, Bewegung, Beschleunigung, Temperatur, Feuchtigkeit und viele andere Parameter.[151]

Sensornetze könnten nicht nur den Feuchtigkeitsgehalt von Blumenbeeten und Rasen überprüfen und automatisch die Sprinkleranlage in Gang setzen oder den Verantwortlichen an dringende Maßnahmen erinnern.[152] Sie könnten zum Beispiel auch die physische Belastung und Witterungsbeanspruchung von Brücken, Stromversorgungssystemen und Bauwerken beobachten, den Straßenzustand überwachen und präzis den Straßenbereich benennen, auf dem sich Glatteis gebildet hat, oder in einem zugangsgeschützten Bereich verdächtige Bewegungen wahrnehmen und an die zuständige Kontrollstelle melden. Sensornetze

[150] S. z.B. Mattern 2003c, 18; Mattern 2007a, 14.

[151] S. oben 36 f.

[152] Mattern 2007a, 15, der eine Geschichte von Christoph Podewils nacherzählt.

könnten im industriellen Bereich zur umfassenden Überwachung komplexer Prozesse und Anlagen, etwa chemischer Großanlagen, eingesetzt werden. Im Maschinenbau könnten sie zum Beispiel den Materialfluss, den Werkzeugstand und andere Prozesskennzahlen erheben und dadurch helfen, die komplexen Betriebsmittelkreisläufe und -durchsätze besser zu beherrschen.[153] Sie könnten die Luftqualität kontrollieren, Brände melden oder Fehlfunktionen von Komponenten erkennen. Sie könnten schließlich dazu beitragen, im Umweltbereich das Verursacherprinzip bei Umweltbelastungen durchzusetzen oder gar Umweltdelikte zu erkennen und dem Verursacher zuzuordnen.[154]

Sensornetze können aber nicht nur Naturphänomene oder den Zustand von Gegenständen beobachten, sondern auch direkt oder indirekt das Verhalten von Menschen oder Gruppen.[155] Dies gilt nicht nur für die Verkehrsüberwachung oder die Kontrolle von Hochsicherheitsbereichen. Die unbemerkte, räumlich und zeitlich vollständige Überwachung durch Sensornetze kann grundsätzlich auch für beliebige andere Zwecke eingesetzt werden.[156]

1.3.4 Haustechnik

Ein potentiell wichtiges Anwendungsfeld der allgegenwärtigen Datenverarbeitung ist ihre Nutzung in Gebäuden. Hierbei geht es weniger um den vielfach als Beispiel strapazierten »intelligenten Kühlschrank«, der selbsttätig Bier nachbestellt, wenn der Vorrat zu Neige geht. Zu erwarten ist vor allen Dingen, dass die verschiedenen Systeme der Hausinfrastruktur und die großen Geräte im Haus mit Sensoren und Prozessoren ausgestattet und untereinander vernetzt werden. Dies betrifft zunächst die Geräte der klassischen Haustechnik wie Heizung, Lüftung, Klima, Sicherheit und Beleuchtung sowie die Elektro-, Telekommu-

[153] S. z.B. BMBF 2007, 21; Simoneit, in: NEXUS 2005, 112.

[154] S. z.B. auch BSI 2006, 29 f.; UNESCO 2007, 53.

[155] S. z.B. Mattern 2003c, 19.

[156] S. hierzu näher unten 87 ff.

nikations- und Rundfunkgeräte.[157] Weitergehende Vorstellungen beziehen auch weitere Einrichtungsgegenstände wie etwa den Spiegel, der die Bewohner an wichtige Aufgaben erinnert,[158] den Medizinschrank, der selbständig das Verfallsdatum der Medikamente prüft, sowie Türen oder Böden, die Bewegungen erkennen,[159] mit ein. Durch die Vernetzung der Geräte kann vielleicht das Klingeln des Weckers das Licht gedämpft anschalten, die Gardinen oder Rollläden öffnen, die Heizung hoch fahren, eine bestimmte Musik erklingen lassen und die Kaffeemaschine aktivieren. Ein anderes Beispiel ist, dass das Klingeln an der Haustür oder des Telefons die Lautstärke der Musikanlage oder des Fernsehers automatisch senkt.[160]

Die Systeme und Geräte in Büro oder Wohnung sollen sich kontextsensitiv automatisch an die Bedürfnisse der Nutzer anpassen und ihnen Aufmerksamkeit ersparen und Entscheidungen abnehmen. Die Haustechnik erkennt etwa den Nutzer und stellt automatisch die Klima- und Lüftungsanlage auf seine Präferenzen ein.[161] Können beispielsweise RFID-Chips in der Wäsche von einer Waschmaschine gelesen werden, dann kann diese automatisch das richtige Waschprogramm wählen.[162] Sollte sich der Nutzer dennoch um ihre Funktionsfähigkeit kümmern, sind sie mit der Fähigkeit ausgestattet, diese zu erläutern, weitere Informationen über sich zu bieten und Hinweise zur Bedienung, Wartung und Reparatur zu geben.[163]

[157] S. z.B. BSI 2002; Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 72 ff.; Hansen/Fabian/Klafft, in: TAUCIS 2006, 48 ff.; Heesen, in: NEXUS 2005, 150 ff.

[158] S. z.B. Hansen/Fabian/Klafft, in: TAUCIS 2006, 49; Mattern 2007a, 12: Spiegel animiert zu gesundheitsgerechtem Verhalten; BSI 2006, 32: Spiegel bietet Fernsehbild.

[159] S. z.B. oben 36 f. sowie im Folgenden.

[160] S. z.B. Hansen/Fabian/Klafft, in: TAUCIS 2006, 48.

[161] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 72; Hansen/Fabian/Klafft, in: TAUCIS 2006, 48.

[162] Mattern 2007a, 7.

[163] Mit einem NFC-fähigen Mobiltelefon könnte der Nutzer die Selbstdiagnose des defekten Geräts erfahren und sich selbst um Ersatzteile oder den Besuch eines Servicemechanikers kümmern – s. z.B. Langheinrich 2007b, 60.

Stromverbrauchende Geräte sind mit den Computersystemen der Energieerzeuger und -verteiler gekoppelt, um einen unmittelbaren Datenaustausch über Angebot und Nachfrage nach Strom zu ermöglichen. Dies erlaubt, energiesparend Strom zu erzeugen und umgekehrt stromsparend Energie zu nutzen. Jeder Haushalt kann die Preisinformationen der Strombörse abrufen und seinen Stromverbrauch den Preisschwankungen, die an ihn weitergegeben werden, anpassen.[164]

Das Haussicherungssystem kontrolliert selbständig die Ver- und Entriegelung aller verschließbaren Bereiche. Die Eingangsbereiche sind mit Sensoren ausgestattet, die Personen, die die Wohnung betreten wollen, an Hand von biometrischen Merkmalen oder RFID-Tags identifizieren und ihnen je nach Berechtigung den Zutritt erlauben oder verweigern.[165]

Alle Infrastruktursysteme und größeren Geräte sind mit dem Internet verbunden und daher vom Hausbesitzer auch aus der Ferne zu kontrollieren und zu steuern.[166] Wenn etwa die Heizung nicht ohnehin vom elektronischen Terminkalender weiß, wann der Besitzer in das Haus oder die Wohnung zurückkommt, kann dieser, kurz bevor er eintrifft, von unterwegs aus die Heizung hoch stellen. In gleicher Weise kann er die Rollläden ansteuern oder den Inhalt des Kühlschranks abfragen, um zu erfahren, was er auf dem Heimweg noch einkaufen muss. Ebenso können Geräte aus der Ferne gewartet werden, automatische Fehlermeldungen absetzen und den Wartungstechniker mit den für eine Analyse erforderlichen Daten versorgen.[167]

RFID-Chips ohne eigene Energieversorgung in textilen Bodenbelägen ermöglichen Robotern oder anderen mobilen Geräten mit Leseeinheit, die jeweils identifizierbaren Chips zu erkennen und

[164] S. BMBF 2007, 22.

[165] Hansen/Fabian/Klafft, in: TAUCIS 2006, 49.

[166] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 73f.

[167] S. z.B. Hansen/Fabian/Klafft, in: TAUCIS 2006, 49.

dadurch automatisch über den Boden zu navigieren.[168] Durch das Auslesen der einzelnen Chips entsteht beim Roboter eine virtuelle Landkarte, auf der er ein Wegenetz finden kann, das ihn zielgenau zu einem Punkt oder Raum steuert. Ein Lesespeicher wertet aus, welche Stationen bereits angefahren wurden. Indem auf den RFID-Chips Datums- und Zeitangaben hinterlassen werden, kann eine einfache Servicekontrolle durchgeführt werden. Hindernisse werden erkannt und lösen eine spontane Navigationsänderung aus. Besteht das Hindernis nicht mehr, wird auch dieser Bodenbereich wieder angesteuert. Dadurch können zum Beispiel selbsttätige Reinigungsautomaten effizient und energiesparsam ihre Arbeit verrichten oder automatisch gesteuerte Transporteinheiten allein ihren Weg finden.

Für Büros könnten sich Techniken der allgegenwärtigen Datenverarbeitung vor allem für Bürogebäude anbieten, in denen die Nutzer keine festen Plätze oder Räume haben, in denen vielmehr der jeweilige Arbeitsplatz an die Mitarbeiter bedarfsorientiert – vielleicht täglich neu – vergeben wird. In diesem Fall geht es darum, die Arbeitsmittel – Computer- und Telekommunikationseinstellungen, Zugriffsrechte, elektronische Dokumente – jeweils aktuell zur Verfügung zu stellen und die Raumparameter automatisch auf den jeweiligen Nutzer einzustellen. Allgegenwärtige Datenverarbeitung könnte in solchen Umfeldern diese Funktionen erfüllen und zum Beispiel dem Mitarbeiter automatisch seine Telekommunikationsverbindungen auf den in dem Raum verfügbaren Apparat umstellen, die Klimaanlage auf die gewünschte Temperatur einstellen und den Mitarbeitern mitteilen, wo ihr Kollege heute zu finden ist. Um die Behaglichkeit zu erhöhen, werden auch die Lichtstärke und die Lichtfarbe, die Wandfarbe, der Raumgeruch und die Jalousie entsprechend dem hinterlegten Profil eingestellt. Das Wanddisplay zeigt ein Bild aus dem letzten Urlaub.[169]

[168] Vorwerk 2005: Entwicklung von Infineon und Vorwerk.

[169] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 85; Siemoneit, in: NEXUS 2005, 169.

Eine andere Anwendung für Büro- und Produktionsgebäude wird die Zutritts-, Anwesenheits- und Routenkontrolle sein. RFID-basierte Systeme werden nicht nur im Eingangsbereich eingesetzt, sondern auch zu weiteren Zwecken wie die Zeiterfassung, die Zutrittskontrolle zu sicherheitsrelevanten Bereichen, die Prozesskontrolle- und -steuerung und eventuell auch die Leistungskontrolle. Diese Systeme kommen sowohl zur Erfassung von Mitarbeitern als auch von Gästen und Auftragnehmern, die im Gebäude tätig sind, zum Einsatz.[170]

Für Wohnräume ist die Nutzung allgegenwärtiger Datenverarbeitung vor allem zu erwarten, wenn es darum geht, Älteren, Behinderten oder Kranken ein betreutes und technisch unterstütztes Wohnen in ihrem gewohnten Umfeld zu ermöglichen.[171] Bedienungsfreundliche und fehlertolerante Hausanlagen und Haushaltsgeräte sollen diese Nutzer in die Lage versetzen, sich selbst zu versorgen und allein zu leben, ohne sich um Technik kümmern zu müssen. Fehlerfälle werden automatisch abgefangen, etwa indem die Waschmaschine Fehler selbst diagnostiziert und der Werkstatt meldet. Die Bewohner werden bei technischen Abläufen des Alltags unterstützt, etwa durch das automatische Schließen aller Fenster beim Verlassen der Wohnung oder durch das Abstellen bestimmter Geräte wie Herd oder Wasserhahn nach einer bestimmten Frist der Nichtnutzung.[172] Automatisch lässt sich der Rollstuhl an das Bett steuern oder das motorisierte Bett bewegen.[173] Dabei geht es nicht darum, den älteren oder kranken Menschen sämtliche Arbeiten abzunehmen, sondern lediglich den Anteil, der zum vollständigen und sicheren Ausführen der Tätigkeit von der jeweiligen Person nicht mehr erbracht werden kann. Dies ist auf der Basis persönlicher Profile für regel-

[170] S. z.B. BSI 2004, 103.

[171] S. z.B. UNESCO 2007, 44.

[172] S. z.B. Europäische Kommission, o.J.

[173] S. Hansen/Fabian/Klafft, in: TAUCIS 2006, 49.

mäßige Tätigkeiten und einer kontextbasierten Personalisierung für das Reagieren auf spontane Entscheidungen möglich.[174]

Allgegenwärtige Datenverarbeitung soll außerdem ein Tele- oder Home-Monitoring von Gesundheitsparametern oder relevanten Verhaltensweisen ermöglichen, das im Bedarfsfall Hilfe anfordert.[175] Das Monitoring soll ermöglichen, chronisch kranke oder zeitweise gefährdete Menschen zu überwachen oder lange Krankenhausaufenthalte für Patienten zu vermeiden, die sich in erster Linie aus der Notwendigkeit von Langzeitbeobachtungen ergeben. Neben Kosteneinsparungen kann damit eine Steigerung der Lebensqualität der Patienten erreicht werden.

Ansonsten ist zu erwarten, dass Gegenstände mit integrierter Datenverarbeitung nach und nach in die Büro- und Wohnhäuser Einzug halten. Sie werden in dem Umfang gekauft und genutzt werden, wie die Menschen sich durch sie oder durch Dienste, die sie voraussetzen, einen größeren Komfort oder eine gewisse Reputation versprechen. In ihrer Summe und in ihrem Zusammenwirken könnten sie auch für den normalen Haushalt nach und nach zu einer allgegenwärtigen Datenverarbeitung im privaten Umfeld führen.

1.3.5 Verkehrstechnik

Das Kraftfahrzeug und seine Kommunikation mit seiner Umgebung dürfte eines der ersten ernsthaften großen Anwendungsfelder allgegenwärtiger Datenverarbeitung werden. Bereits heute enthalten Autos viele unterschiedliche Sensoren und Mikroprozessoren sowie ein internes Kommunikationsnetz, um Motorwerte, Daten zum Fahrgestell, zu Bremsen, zum Reifendruck, zu weiteren Komponenten und Umgebungsparametern zu messen, auszuwerten und auszutauschen. Sie bewirken selbsttätige Aktionen einzelner Komponenten (Automatische Geschwindigkeitsregelung, elektronische Stabilisierung, Einstellung der Federung, Ein- und Ausschalten der Wischer), die Speicherung von Daten (Protokolle zur Beanspruchung von Komponenten) oder die Ausgabe der Daten in Form von Hinweisen oder Warnungen. Anvancierte Systeme bieten nachtsichtfähige »Assistenten«, die anhand des Bewegungsmusters eigenständig Fußgänger oder Fahrradfahrer ohne Licht erkennen können, lange bevor der Fahrer sie im Dunkeln sehen kann.[176]

Künftig wird die Verbreitung und der Empfang spezifischer Verteildienste wie Fernsehsendungen, Radionachrichten, Verkehrsinformationen, dynamische Routenempfehlungen, Hindernishinweise, Ampelsignale oder Signale aus Polizei- oder Krankenfahrzeugen zunehmen.[177] Dabei könnten etwa von Verkehrsschildern ausgesendete Signale dazu führen, dass im Kraftfahrzeug Reaktionen ausgelöst werden, die etwa das Überschreiten einer zulässigen Höchstgeschwindigkeit oder das Abschalten des Motors auf einen unzulässigen Parkplatz verhindern.[178] Auch umgekehrt, vom Fahrzeug weg, können Meldungen – etwa über einen Unfall oder Stau – verteilt werden und von anderen Kraftfahrzeugen oder Informationssystemen aufgenommen werden.

Daneben werden aber auch interaktive Dienste angeboten und genutzt werden. Neben dem bekannten Mobilfunk könnte ein Internetzugang für Fahrzeuge über das Straßennetz ermöglicht werden, der die einzelnen Fahrzeuge als mobile Netzwerkknoten nutzt.[179] Hierdurch würden vielfältige Dienstleistungen möglich: Zum Schutz des Kraftfahrzeugs gegen Dienstahl oder unberechtigte Nutzung oder zu seinem Wiederfinden wird es identifiziert und lokalisiert. Weiterhin wird die Berechtigung des Fahrers überprüft und das Fahrzeug »freigeschaltet«.[180] Zur Teleüber-

[174] S. BSI 2006, 63.

[175] S. z.B. BSI 2006, 32f., 34f.; Hansen/Fabian/Klafft, in: TAUCIS 2006, 52.

[176] S. z.B. BSI 2006, 83; Hansen/Fabian/Klafft, in: TAUCIS 2006, 45; BMBF 2007, 21.

[177] S. z.B. Herrtwich/Rehborn/Franz/Wex 2006, 133 ff.

[178] S. hierzu z.B. www.vision-zero.com; BSI 2006, 84. Zwangsabbremsungen lehnen die Fahrzeughersteller bisher ab – s. z.B. Herrtwich/Rehborn/ Franz/Wex, 138f.

[179] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 79; BSI 2006, 83f.

[180] S. z.B. Herrtwich 2003, 67, 73; Hansen/Fabian/Klafft, in: TAUCIS 2006, 46.

wachung von Sicherheitsfunktionen im Kraftfahrzeug werden die Daten von bestimmten Komponenten erhoben und an den Hersteller oder die Werkstatt geschickt. Umgekehrt erhält der Fahrer aufgrund dieser Daten rechtzeitige Hinweise zu Inspektionen, Verschleißerscheinungen, Unregelmäßigkeiten, dringenden Reparaturen oder zur Fahrweise.[181] Soweit eine Komponente austauschbare Software enthält, kann sie sogar aus der Ferne gewartet werden, indem neue Software-Updates geladen werden.[182] Diese können auch neue Funktionalitäten und neue Anwendungen im Fahrzeug ermöglichen.[183] Schließlich können über das Internet weitere Informationen über Funktionen des Kraftfahrzeugs aufgerufen werden oder eine individuelle und dynamische Routenführung angefordert werden, die aktuelle Verkehrsinformationen berücksichtigt.

Das Auto erhält »Augen und Ohren«. Sie ermöglichen, um das Auto einen virtuellen »Sicherheitsbereich« zu errichten. Um Unfälle oder Beschädigungen zu vermeiden, sorgen Abstandsradar und Abstandssensoren dafür, dass das Auto sich anderen Kraftfahrzeugen oder Hindernissen je nach Geschwindigkeit nicht mehr als 20 m bis 20 cm nähert.[184] Auf geeigneten Abschnitten der Autobahnen können Autopiloten die Lenkung des Fahrzeugs übernehmen.[185] Dies erlaubt sogar Kolonnenfahren auf der Autobahn. NFC sorgt dafür, dass andere Fahrzeuge, Ampeln und Verkehrsschilder frühzeitig wahrgenommen werden.

Die Hersteller werden diese Zusatzdienste zum Kraftfahrzeug anbieten, um ihr Produkt anzureichern und interessanter zu machen, um besser über das Kraftfahrzeug und seinen Halter oder Fahrer informiert zu sein und um die Kundenbetreuung zu verbessern und die Kundenbindung zu stärken.

[181] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 79; Herrtwich 2003, 74.
[182] S. z.B. Herrtwich/Rehborn/Franz/Wex 2006, 138f.
[183] S. hierzu z.B. Herrtwich 2003, 73f.
[184] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 79; BMBF 2007, 21
[185] S. Hansen/Fabian/Klafft, in: TAUCIS 2006, 47.

Aber nicht nur die Hersteller, auch weitere Anbieter sind an den neuen Geschäftsmöglichkeiten, die allgegenwärtige Datenverarbeitung rund um das Kraftfahrzeug bietet, interessiert. Wenn ein Dienst den Standort des Kraftfahrzeugs kennt, kann er den Fahrer oder die anderen Insassen nach deren Situation und Interessen über andere Kraftfahrzeuge, Menschen, Sehenswürdigkeiten, Restaurants, Einkaufsmöglichkeiten, Werkstätten und ähnliche Orte oder Gelegenheiten in der Nähe des Standorts informieren.[186] Mit Raststätten, Tankstellen, Werkstätten oder Hotels könnten so bidirektionale Verbindungen hergestellt und Essen, Reparaturen oder Übernachtungen gebucht werden.

Die Kraftfahrzeuge der Zukunft werden auch untereinander Daten, insbesondere zum aktuellen Verkehrsgeschehen, austauschen. Indem sie mittels sich ad hoc strukturierender Netzwerke eine direkte Kommunikation zwischen den Fahrzeugen aufbauen, werden sie zu »lernfähigen Schwarmkomponenten eines dezentralen Kommunikations- und Sensornetzwerks«.[187] Hat eines ihrer Assistenzsysteme eine auch für andere Assistenzsysteme relevante Feststellung oder Entscheidung getroffen, teilt sie dies an die Kraftfahrzeuge in der näheren Umgebung mit, die diese verarbeiten und für eigene Entscheidungen nutzen, über die sie ihrerseits andere Systeme informieren. Auf diese Weise können zum Beispiel Warnungen vor Fußgängern, Nebelbänken, Blitzeis oder Auffahrunfällen – in Sekundebruchteilen von einem Fahrzeugsystem zum nächsten weitergeleitet werden. Dadurch kann der Fahrer über starke Bremsvorgänge anderer Fahrzeuge unterrichtet werden, auch wenn er diese nicht sehen kann, und dadurch frühzeitig vor Gefahrensituationen gewarnt werden. Auf diese Weise können aber auch spezifische verkehrsfluss- oder ortsabhängige Hinweise und Tipps ausgetauscht werden.[188]

[186] S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 80; Herrtwich 2003, 71f.
[187] BSI 2006, 28, 84; Network on Wheels 2005.
[188] BSI 2006, 27f., 83 ff.

1.3.6 Logistik

Ein zweites großes Anwendungsfeld allgegenwärtiger Datenverarbeitung wird die Logistik sein. Allgegenwärtige Datenverarbeitung verspricht, den Medienbruch zwischen realer und digitaler Welt zu verhindern und die kostspielige Lücke zwischen Informationssystem und Realität zu schließen.[189] Der Mensch als Mediator zwischen beiden Welten kann entfallen. Er muss nicht mehr die reale Welt beobachten und sie in Form von Daten in der digitalen Welt abbilden, indem er diese erhebt, eingibt und pflegt. Die Informationstechnik kann mit allgegenwärtiger Datenverarbeitung diese Daten selbst erheben. Dadurch wird die Datenverarbeitung aktuell und weniger fehleranfällig. Werden die Daten an den Gegenständen mitgeführt, erlaubt dies auch Delegation von Aufgaben und Entscheidungen an teilautonome Prozesse.[190]

Wenn Produkte über RFID-Chips ihre individuelle Identität jedes Mal automatisch preisgeben, wenn sie das Tor einer Lagerhalle oder die Laderampe eines LKWs passieren, dann kann ohne manuelles Zutun eine nahezu lückenlose Verfolgung der Warenströme über die gesamte Lieferkette hinweg sichergestellt werden. Dies ermöglicht, die Lagerhaltung zu reduzieren, die Verteilung der Güter über Raum und Zeit zu optimieren,[191] Liege- oder Stillstandszeiten zu verringern, nicht lieferbare Produkte zu identifizieren, Schwund und Diebstahl präzise festzustellen sowie das gesamte Produktions- und Produktmanagementsystem zu erneuern. Künftig wird es möglich sein, die physische Realität mit der Abbildung in den betrieblichen Informationssystemen so zu vernetzen, dass Veränderungen in der Realität automatisch in Echtzeit in den Informationssystemen dargestellt werden. Damit können Managementsysteme schnell und effektiv auf betriebliche Veränderungen reagieren. Inventuren, Prozesskennzahlen und Fehleranalysen sind »auf einen Click hin« möglich.[192]

Die Standardisierungsorganisationen der europäischen und US-amerikanischen Konsumgüterindustrie haben sich für Konsumgüter auf einen »Electronic Product Code (EPC) geeinigt, der zur Identifizierung eines Produkts in RFID-Systemen genutzt werden soll.[193] EPC sieht für den Regelfall einen einfachen RFID-Tag vor, der die weltweit einmalige Identitätsnummer des Logistikobjekts speichert, während die Daten zu dem Objekt im Hintergrund in Datenbanken bereitgehalten werden.[194] Das EPCglobal Network ermöglicht die Zusammenführung dieser Daten durch den »Object Name Service (ONS)«, der mitteilt, wo Daten zu dem entsprechenden Product Code zu finden sind. Die Produktangaben werden in der standardisierten »Physical Markup Language (PML)« beschrieben. Das Softwaresystem »Savant« verwaltet und transportiert diese Daten.[195]

Die Identifizierung des jeweiligen Produkts erlaubt, dessen Geschichte zu dokumentieren. Vielfach ist eine solche Rückverfolgbarkeit vorgeschrieben,[196] sinnvoll oder zumindest hilfreich. Durch die Identifizierung kann etwa festgestellt werden, wer ein Produkt an welchem Tag hergestellt hat, wann es ausgeliefert worden ist, ob es immer ausreichend gekühlt war, wann es vielleicht unverträgliche Stöße abbekommen hat, wer es gekauft hat, wo es genutzt und wie es entsorgt worden ist.[197] Bestimmte Er-

189 S. z.B. Fleisch/Christ/Dierkes 2005, 3 ff.

190 S. z.B. Simoneit, in: NEXUS 2005, 110.

191 Das richtige Material zur richtigen Zeit am richtigen Ort.

192 S. näher Fleisch/Christ/Dierkes 2005, 9 ff.; Winand/Frankfurt 2007, 78 ff.; Coroama u.a. 2003, 20 ff.; Simoneit, in: NEXUS 2005, 111, 176; acatech 2006, 10; Artikel-29-Datenschutzgruppe 2005a, 5; AK Technik 2006, 21f.; Van de Voort/Ligtvoet 2006, 3 ff.; UNESCO 2007, 41.

193 S. z.B. Müller/Handy, DuD 2004, 655; Flörkemeier 2005, 87 ff.

194 S. z.B. Artikel-29-Datenschutzgruppe 2005a, 14; Thiesse 2005a, 101 ff.; BSI 2006, 27.

195 Müller/Handy, DuD 2004, 655.

196 Bei Lebensmittel wird die Rückverfolgbarkeit z.B. von Art. 18 der EG-Verordnung 178/2002 gefordert.

197 S. z.B. BMBF 2007, 21; Coroama u.a. 2003, 20; s. zur Nutzung in Medizin und Pharmazie Voort/Ligtvoet 2006, 10 ff.

eignisse – etwa drohender Ablauf der Haltbarkeit – könnten zu automatischen Preissenkungen führen, um das Produkt dem gesunkenen Warenwert entsprechend noch verkaufen zu können.[198] Auf der Grundlage solcher Daten können auch neue Konzepte für individuelle Wartungs-, Rückruf- und Entsorgungsprozesse realisiert werden.[199]

Die Identifizierungsmechanismen ermöglichen auch festzustellen, ob es sich bei dem Produkt um ein Original handelt. Dies ist in der Luftfahrtbranche vorgeschrieben und in der Pharmabranche empfohlen, um Produktfälschungen erkennen und abwehren zu können.[200] In allen anderen Branchen könnte dies ein Instrument sein, um Produktpiraterie bekämpfen zu können. Viele Geräte würden dann Austauschteile nur noch bei Vorhandensein eines auf dem RFID-Tag gespeicherten Autorisierungsschlüssels akzeptieren. Dadurch könnten Plagiate von Ersatzteilen erkannt und vom Markt verdrängt werden. Diese Technik könnte aber auch angewendet werden, um Kunden an bestimmte Marken zu binden. So könnten Rasierapparate, Drucker und Fotoapparate nur noch Austauschteile vom gleichen Hersteller akzeptieren oder Waschmaschinen nur noch mit Pellets bestückt werden, die eingepresst einen »richtigen« Einweg-RFID enthalten.[201]

Noch weitergehend könnte mit solchen Techniken auch die Lizenzierung von Produkten für bestimmte Nutzungen oder für eine bestimmte Zeit überwacht werden. Beispielsweise könnten Autos ein RFID-System enthalten, das die Originalität und das Alter von Ersatz- und Austauschteilen, wie zum Beispiel Reifen, automatisch überwacht. In Vertragswerkstätten würden Teile, die eine vom Hersteller vorgegebene Maximallebensdauer erreicht haben oder deren Nutzungslizenz erloschen ist, erkannt und gewechselt. Es könnten nur Austauschteile von lizenzierten

198 S. z.B. Coroama u.a. 2003, 21, 25, 110; AK Technik 2006, 22.

199 S. z.B. BSI 2006, 27f.; Mattern 2003c, 26 ff.; acatech 2006, 10.

200 S. z.B. Voort/Ligtvoet 2006, 11; Artikel-29-Datenschutzgruppe 2005a, 4f.; Hansen/Fabian/Klafft, in: TAUCIS 2006, 50; Holznagel/Bonnekoh 2006, 15.

201 BSI 2004, 102.

Herstellern eingebaut werden. Der Bordcomputer würde diese anhand ihrer verschlüsselten ID prüfen und akzeptieren. Ohne eine noch gültige ID verweigert das Fahrzeug die Funktion.[202]

In Produktion und Distribution könnte die Identifizierung des Gegenstands und seine Verknüpfung mit weiteren Informationen genutzt werden, um neue Steuerungskonzepte zu etablieren. Ein Großteil der Steuerungsfunktionen könnte in das einzelne Werkstück oder Produkt verlagert werden. Dadurch könnte statt einer zentralen Produktionsplanung eine dezentrale Materialflusssteuerung realisiert werden.[203] Fertigungs- und Distributionsprozesse wären vermutlich weniger fehleranfällig.[204] Die Verfügbarkeit von Kontextinformation, wie etwa über den Ort, den Inhalt, den Zustand oder die Nachbarschaft eines Containers, könnte künftig sogar dafür genutzt werden, dass sich logistische Prozesse weitgehend selbst steuern.[205]

Der Kunde kann von der Identifizierung und Lokalisierung eines Produkts ebenfalls Vorteile haben: Über die Web-Seite des Produkts kann er zusätzliche Informationen einholen, und kann eventuell erfahren, wann es hergestellt worden ist und was ihm bisher widerfahren ist. Durch zusätzliche Angaben des Herstellers oder Verkäufers oder Dritter wie »Stiftung Warentest« kann die Information des Verbrauchers erheblich verbessert werden.[206] Sein Einkauf kann – ohne, dass die Waren aus dem Einkaufswagen oder -korb ausgepackt werden müssen und damit ohne Schlangestehen – automatisch abgerechnet werden.[207]

Wenn Produkte auch noch nach dem Verkauf mit dem Unternehmen online in Kontakt bleiben und Daten über ihre Umgebung und Nutzung erfassen, erlaubt dies dem Unternehmen wertvolle

202 BSI 2004, 102.

203 Simoneit, in: NEXUS 2005, 110, 177; BSI 2006, 27.

204 S. z.B. BSI 2006, 26; Winand/Frankfurt 2007, 79f.

205 COBIS o.J.; Fleisch/Christ/Dierkes 2005, 22 ff.; Rothermel 2007, 36; Siemoneit, in: NEXUS 2005, 122.

206 Siemoneit, in: NEXUS 2005, 218; Roßnagel 2004, 341f.

207 S. z.B. Mattern 2007a, 7; Coroama u.a. 2003, 21f.; Roßnagel/Müller, CR 2004, 626f.

Rückschlüsse auf die Entwicklung und Konzipierung neuer Produkte, gezielte Werbung im Sinn von Cross-Selling und One-to-One-Marketing und das Anbieten zusätzlicher Dienstleistungen.[208]

Auch nach dem Kauf kann die Identifizierung und Lokalisierung des Gegenstands weiter genutzt werden – beispielsweise für Kommunikation mit anderen Gegenständen im Rahmen eigener privater oder gewerblicher Ubiquitous Computing-Anwendungen. Sie erleichtern das Wiederfinden des Gegenstandes, wenn er verloren gegangen ist, ermöglichen eine Verwaltung eigener Gegenstände, lassen einen Folgeservice zu, wie etwa bei Kleidung die automatische Auswahl passender Accessoires, und erleichtern Reklamationen oder Reparaturen.[209] Um Täuschungen zu bekämpfen, werden die Rücknahme- oder Garantiepflichtigen darauf achten, ob tatsächlich der von ihnen an diesen Kunden gelieferte Kaufgegenstand vorgelegt wird.[210]

Der flächendeckende Einsatz von RFID zur Produktkennzeichnung könnte auch zwei großen Problemen der Abfallverwertung und -beseitigung abhelfen.[211] Zum einen könnte die Identifizierung eines Produkts in automatisierten Prozessen Aufschluss über Produktzusammensetzung, Produktaufbau, umweltschädliche Komponenten und wiederverwertbare Rohstoffe sowie konkrete Hinweise zur Abfallbehandlung wie Demontageanleitungen und Gefahreneinstufungen geben.[212] Dies verspricht eine Effizienzsteigerung, höhere Sortenreinheit und verbesserten Arbeitsschutz im Wiederverwertungsprozess. Zum anderen ließen sich über die Kennzeichnung Hersteller, Importeure, Verkäufer und Eigentümer feststellen und für Recycling und Entsorgung in die Verantwortung nehmen.[213] Dadurch könnte der illegalen Entsorgung von Abfällen vorgebeugt und das umweltrechtliche und -politische Grundproblem der »gerechten« Verteilung der Kosten einer Lösung zugeführt werden.

Darüber hinaus ergeben sich Chancen aus der kontinuierlichen Verknüpfung mit Hintergrundsystemen.[214] So ließe sich etwa die Produktgeschichte (Hersteller, Herstellungsdatum, Produktionskosten) erfassen, dynamische ökonomische Informationen (Produktpreis, Recyclingkosten, Materialwert) festhalten und speichern, welchen Umwelteinflüssen ein Produkt ausgesetzt ist oder wer zu welchem Zeitpunkt erforderliche Wartungs- oder Reparaturarbeiten vorgenommen hat.

Die Abfallerkennung mittels RFID könnte zum einen bei Massenwaren des täglichen Gebrauchs an die RFID-Infrastruktur anknüpfen, die bei Produktion und Vertrieb »ohnehin« entstehen wird. Hier sind erhebliche Synergieeffekte zu erwarten, da die RFID-Chips bereits auf den Produkten angebracht sein werden und die Datenverarbeitungssysteme im Recyclingbereich lediglich mit entsprechenden Informationen über die den Chips zugeordneten Produkte versorgt werden müssen. Zum anderen könnten RFID-Chips auch speziell für die Entsorgung angebracht werden. Dies erscheint allerdings gegenwärtig wohl nur im Bereich von Industrie- und Großgeräten realistisch.

Technische Identifikatoren können helfen, Zeit zu sparen und Bequemlichkeit zu erhöhen. Zugleich können sie für diejenigen, die Identifizierungs- und Kontrollaufgaben haben, den notwendigen Aufwand für die Vorbereitung, die Implementation und den Unterhalt der Identifikations- und Kontrollsysteme signifikant reduzieren. So können kontaktlose Zugangs- und Kontrollsysteme den bequemen Zugang zu Gebäuden, Freizeitanlagen, Theatern, Kinos, Stadien, Museen und Bibliotheken gewährleisten sowie eine belästigungsfreie Kontrolle von Pässen, Ausweisen, Kundenkar-

208 S. z.B. Pfaff/Skiera 2002, 32f., 35f.; Siemoneit, in: NEXUS 2005, 179.

209 S. z.B. Pfaff/Skiera 2002, 36; Mattern 2007a, 18; Langheinrich 2005a, 355; Langheinrich 2007a, 135; Müller/Handy, DuD 2004, 658.

210 S. z.B. Siemoneit, in: NEXUS 2005, 212.

211 S. Siemoneit, in: NEXUS 2005, 219; aus der Sicht der Abfalltechnik Urban/Morgan/Kuhnhenn 2006, 86 ff.; s. auch Mattern 2007a, 7.

212 Urban/Morgan/Kuhnhenn 2006, 90 ff.; Morgan/Urban/Kuhnhenn 2006, 124 ff.

213 Kuhnhenn/Urban/Morgan 2006, 113 ff.

214 S. z.B. Mattern 2003c, 12.

ten an Grenzen, Mautstationen und Verkaufstheken ermöglichen. In Bussen und Bahnen kann zum Beispiel mit Mobiltelefonen mit NFC-Technologie kontaktlos der jeweils günstigste Fahrpreis automatisch abgebucht werden.[215]

1.3.7 Wearable Computing

Ubiquitous Computing wird nicht nur in die nähere Umgebung des Menschen, wie Haus oder Auto, eindringen, sondern auch in die Hülle um seinen Körper oder sogar in diesen selbst.[216] Immer mehr elektronisches Gerät wird in miniaturisierter Form in Kleidung, Armbanduhren, Brillen und Schmuckstücke eingebaut sein.[217] Ihre Aufgaben werden vor allem sein, die Sicherheit des Nutzers zu erhöhen, seine Sinne zu erweitern und sein Gedächtnis zu unterstützen. Die Sicherheit des Nutzers wird zum Beispiel dadurch erhöht, dass seine Körper- und Umgebungsdaten erfasst und verarbeitet werden. Die Sicherheit des Anwenders wird erhöht, wenn durch Chips in der Kleidung der Aufenthaltsort jedes Mitarbeiters oder jedes in einem Bereich befindlichen Menschen festgestellt werden kann.[218] Ein anderes Beispiel könnte eine Alarmfunktion sein, die Gegenstände in Jacke oder Hose vor Diebstahl schützen.[219] Wearable Computing wird die Sinne des Nutzers verstärken, indem Sensoren ihn unterstützen, die Umgebung wahrzunehmen. Schließlich werden die kleinen tragbaren Rechner sein Gedächtnis erweitern, indem ihm Informationen über Kopfhörer oder über die oben vorgestellte Brille[220] präsentiert werden, die direkt auf die Netzhaut projiziert werden. So kann der Benutzer eine auf seine persönliche Interessenlage

215 S. z.B. Langheinrich 2007, 58 ff. mit Beispielen aus Hanau und Japan.
216 S. zu Implantaten z.B. Sietmann, c't 2004/16, 85 ff.; UNESCO 2007, 43f.
217 S. hierzu auch Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 96 ff.
218 S. die Beispiele in UNESCO 2007, 42f.
219 S. z.B. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 97.
220 S. oben 39.

zugeschnittene »Informations- und Funktionsaura« mit sich herumtragen, die ihn zugleich mit der Welt verbindet.[221]

Reporter, Wartungsmonteure, Lagerarbeiter und ähnlich Beschäftigte benötigen die Hände frei und dennoch situations- und kontextabhängig vielfältige Informationen. Für sie wäre es sehr hilfreich, wenn die sie umgebenden Datenverarbeitungssysteme erkennen könnten, welche Information sie benötigen, und diese ihnen über spezifische Ausgabegeräte, wie zum Beispiel die Projektion von Schaltplänen direkt auf das zu reparierende Systemteil, ausgeben.[222]

Wearable Computing kann außerdem neuartige Interaktionsformen zwischen Mensch und Technik nutzen. Beispielsweise können die Fasern von Kleidungsstücken beim Dehnen ihren elektrischen Widerstand ändern. Dadurch können Körperbewegungen erfasst und die so gewonnenen Daten für vielfältige Zwecke genutzt werden – etwa um mit ihnen Funktionen von Geräten auszulösen.[223]

Für die ambulante Beobachtung von Patienten sind bereits viele Prototypen von Kleidungsstücken wie Hemden oder Anzüge entwickelt worden,[224] in die sowohl verschiedene Sensoren als auch Speicher- und Kommunikationseinheiten integriert sind, die Vitalparameter wie Blutdruck, Herzfrequenz oder Sauerstoffverbrauch erfassen und an eine Kontrollstation übermitteln können. Durch diese Kleidungsstücke können auch Alarme ausgelöst werden, wenn die gemessenen Werte dazu Anlass geben.

Der Nutzer könnte seinen Computer in der Zukunft generell als »Wearable« nutzen. Der eigentliche Computer ist nicht größer als eine Kreditkarte und wird in der Kleidung getragen. Er steht mit den Ein- und Ausgabemedien über ein Body Area Network in

221 Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 98f.
222 Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 98; Siemoneit, in: NEXUS 2005, 169.
223 S. Mattern 2003c, 13.
224 S. hierzu näher BSI 2006, 35f.; BMBF 2007, 21.

Verbindung. Der sichtbare Teil des Computers ist eine Brille mit Retinaldisplays. In ihr sind außerdem auch Mikrofon, Kamera, Stereoton und GPS-System integriert. Weitere Sensoren ermitteln die Kopfposition des Brillenträgers, inklusive Blickrichtung und Kopfneigung, so dass der PC stets weiß, wohin der Benutzer gerade sieht. Der Brillen-PC der Zukunft kombiniert Mobiltelefon, Fotoapparat und Videokamera und ist ständig mit dem Internet verbunden. Die Eingabe von Informationen über Tastatur und Mausklicks wird ersetzt durch Sprach- und Gestenerkennung. Die Brille kann aber auch eine virtuelle Tatstatur auf den Tisch, an die Wand oder auf andere geeignete Unterlagen projizieren.[225]

Die wohl gewichtigsten Veränderungen kann die kleine Kamera verursachen, die in die Brille beinahe unsichtbar integriert ist. Sie erweitert den Sehsinn des Nutzers, indem dieser durch sie im Infrarotmodus auch in der Nacht sehen, durch die Zoomfunktion wie mit einem Feldstecher auch ferne Dinge erkennen oder im Makromodus wie durch eine Lupe kleine Strukturen wahrnehmen kann.[226] Da die Kamera in die Brille integriert ist, sieht sie genau das, was der Träger sieht. Das kann dieser dazu verwenden, alles, was sich vor ihm akustisch oder visuell abspielt, aufzuzeichnen. Diese Aufzeichnungen können durch Orts- und Zeitstempel markiert und so leicht wieder gefunden werden. Die Daten werden auf den individuellen Server des Nutzers übertragen und dort als »Tagebuch der Sinne«[227] gespeichert. Mit geeigneter Software kann so jeder Moment im Leben in Erinnerung gerufen werden.

Sollte der Speicherplatz Probleme bereiten oder an einem umfassenden »Tagebuch« kein Interesse bestehen, kann ein System wie »DejaView« verwendet werden. Bei diesem ist die Kamera in Dauerbetrieb, zeichnet aber die Bilder nur auf einen Chip, der sie je nach Einstellung rollierend einen gewissen Zeitraum – die letzten 30 Sekunden oder 30 Minuten – speichert. Durch Knopfdruck wird die Aufnahme nicht mehr überschrieben, sondern auf den Server übertragen und steht dort als Beweismittel (etwa ein Unfall) oder als Erinnerungsschnipsel (eine schönes Erlebnis, eine besondere Peinlichkeit) zur Verfügung.[228]

Begegnet man einem Menschen, wird man künftig von ihm ein Bild oder einen Videoausschnitt aufnehmen und dazu die elektronisch ausgetauschte Visitenkarte abspeichern. Trifft man ihn irgendwann wieder, erkennt die Bilderkennungssoftware, um wen es sich handelt, und das Retinaldisplay zeigt an, wer er ist und wann man ihn das letzte Mal gesehen hat – und eventuell auch, was man sonst über ihn wissen muss.[229] Die Erinnerungsfunktion kann auch beim Erkennen eines Gegenstands helfen, bestimmte mit ihm verbundene Aufgaben nicht zu vergessen.[230]

1.4 Szenarien

Um sich vorstellen zu können, wie solche Anwendungen zusammenwirken und das Leben in einer Welt der allgegenwärtigen Datenverarbeitung bestimmen können, empfiehlt es sich, Lebensausschnitte in Form von Zukunftsbildern zu beschreiben. Sie sind keine Prognosen der Zukunft, sondern versuchen in einem Gedankenexperiment in sich stimmige Ausschnitte aus möglichen Zukünften darzustellen.[231] Sie beschreiben Handlungssituationen und Handlungszusammenhänge, in denen Techniken der allgegenwärtigen Datenverarbeitung genutzt werden könnten.[232] Da die folgenden Szenarien darauf zielen zu erkennen, welche Chancen und Risiken Techniken der allgegenwärtigen Datenverarbeitung bieten, und vor allem herauszufinden, wo Verzweigungssituationen bestehen, die es ermöglichen, auf

225 S. Maurer, Informatik-Spektrum 2004, 46; Mattern 2007a, 13.
226 S. Maurer, Informatik-Spektrum 2004, 46.
227 S. Maurer, Informatik-Spektrum 2004, 47.
228 S. Maurer, Informatik-Spektrum 2004, 48.
229 S. Maurer, Informatik-Spektrum 2004, 49.
230 S. hierzu die Beispiele in Satyanarayanan 2001.
231 Allgemein zur Prognosefähigkeit und Zielsetzung von Szenarien Roßnagel 1993, 105 ff.
232 S. z.B. Hubig, in: NEXUS 2005, 2 ff.

die Entwicklung der Zukunft durch Technik- und Rechtsgestaltung Einfluss zu nehmen, handelt es sich um technikinduzierte Trend-Szenarien.[233]

Viele der in Szenarien beschriebenen Anwendungen[234] werden vielleicht in dieser Weise nie realisiert werden. Umgekehrt werden Anwendungen kreiert werden, die heute noch nicht vorstellbar sind. Jedoch darf man davon ausgehen, dass viele Anwendungen sich der im Feld des Ubiquitous Computing verwendeten Technologien bedienen werden.[235] Für oder gegen diese soll in den Szenarien keine Partei ergriffen werden. Vielmehr sollen die Szenarien als mögliche gemeinsame Grundlage einer Diskussion über die Frage, wie möchten wir in Zukunft leben, dargestellt werden.[236]

1.4.1 Zugreise

Ein Beispiel für die künftige Nutzung von Ubiquitous Computing könnte das Reisen sein.[237] Dem Zugreisenden werden schon in der Nähe des Bahnhofs Informationen über Verspätungen, Gleisänderungen oder Ersatzverbindungen übermittelt. Diese könnten ihm je nach Einstellung auf einem Display angezeigt oder akustisch (etwa über einen kleinen Lautsprecher im Ohrring[238]) ausgegeben werden. So muss er sich nicht beeilen, wenn er weiß, dass der Zug

[233] S. hierzu und anderen Formen von Szenarien für die rechtwissenschaftliche Technikfolgenforschung Roßnagel 1993, 119 ff., 148 ff.

[234] S. z.B. TA Swiss 2003, 46 ff.; Coroama u.a., 2003, 11 ff.; Hansen/Fabian/Möller/Spiekermann, in: TAUCIS 2006, 137 ff.; NEXUS 2005, 107 ff.

[235] Zu den vielfältigen wirtschaftlichen und sozialen Voraussetzungen und Bestimmungsfaktoren s. TAUCIS 2006, 63 ff. und Heesen, Simoneit und Wiegerling, in: NEXUS 107 ff.

[236] S. zur Diskussion wirtschaftlicher, sozialer und individueller Folgen insbesondere NEXUS 2005, 107 – 308.

[237] S. näher Coroama u.a. 2003, 81 ff.; Roßnagel/Müller, CR 2004, 627; Roßnagel 2004, 341f.; Wiegerling, in: NEXUS 2005, 231 ff.

[238] Zu Wearable Computing und sogar der Vision einer digitalen Aura s. Behrendt/Erdmann/Würtenberger, in: TA Swiss 2003, 97.

einige Minuten Verspätung hat. Hat der Zug eine größere Verspätung kann er sich ein wenig im Shoppingbereich des Bahnhofs umsehen. Sofern er die Zeit nutzen will, kann ihn sein Endgerät daran erinnern, dass er noch Rasierschaum und Rasierklingen kaufen muss, und ihn direkt zur Drogerie im Bahnhof führen. Die Empfehlung, einen neu erschienen Roman zu kaufen, die ein anderer Reisender virtuell am Schaufenster einer Buchhandlung hinterlassen hat und die er im Vorbeigehen mit seinem Endgerät zur Kenntnis nimmt, kann er nicht mehr befolgen, da sein Zug bald ankommt.

In einem unbekannten Bahnhof kann er sich durch einen Navigationsdienst, den er auf seinem persönlichen Endgerät empfängt, direkt zum Abfahrtsgleis und dem Ort führen lassen, an dem der Wagen mit seinem reservierten Sitz halten wird. Hat er keinen Sitzplatz reserviert, wird er im Zug von dem Navigationssystem zu dem nächsten für seine Reiseroute und seine Präferenzen (Nichtraucherplatz am Fenster mit Tisch) passenden freien Platz geleitet. Beim Einsteigen wird die elektronische Fahrkarte automatisch gelesen.

Hat der Zug Verspätung oder werden gar Anschlusszüge verpasst, wird dies nicht nur per Lautsprecher den Reisenden durchgesagt, sondern auch vom Zuginformationssystem den persönlichen Endgeräten der Nutzer mitgeteilt. Diese suchen und reservieren eine zur Verspätung passende Ersatzverbindung und zeigen sie dem Reisenden an. Sie klären zudem die Auswirkungen der Verspätung auf den Terminplan des Reisenden und fragen ihn, ob sie entsprechende Nachrichten an die Personen absetzen sollen, mit denen er verabredet ist. Sie buchen außerdem das für den Zielort bestellte Taxi auf die neue Ankunftszeit um. Das Zuginformationssystem überträgt die automatisch erstellte Bestätigung der Verspätung auf das mobile Endgerät des Reisenden. Die ihm hierfür zustehende Rückerstattung kann er sich bei der nächsten Buchung verrechnen lassen.

Am Zielbahnhof angekommen kann er sich den Weg zum Taxistand anzeigen lassen. Andere Reisende nutzen die Hinweise zum nächsten Angebot für Mietfahrräder oder zu den Haltestellen des öffentlichen Nahverkehrs. Straßen- oder U-Bahnen melden beim Anfahren an die Haltestelle dem Reisenden ihre Endstation und die bis dahin noch anzufahrenden Stationen. Das mobile Endgerät kann dadurch signalisieren, ob dies die richtige Bahn ist, und seinen Nutzer auch später darauf aufmerksam machen, wann er aussteigen muss.

1.4.2 Einkaufen

Das Einkaufen im Supermarkt wird künftig stark von der Technologie der RFID-Systeme beeinflusst sein.[239] Bereits heute erproben dies Lebensmittelketten, indem sie Produkte, bei denen der Warenwert dies rechtfertigt, mit einem RFID-Tag ausstatten.[240] Dieser ermöglicht sowohl die eindeutige Identifizierung des einzelnen Produkts als auch das Abspeichern weiterer produktbezogener Informationen.

Der Kunde nutzt einen Einkaufswagen, der mit einem Klein-Computer, einem RFID-Leser und einem Display ausgerüstet ist. Sein persönliches Gerät übermittelt seine Einkaufsliste an den Einkaufswagen. In dessen Display wird angezeigt, welche Waren verfügbar sind und welche Waren der Supermarkt als Alternative empfiehlt, weil er das spezifische Produkt nicht vorrätig hat. Außerdem werden die verfügbaren Artikel auf der Einkaufsliste dem Weg durch den Supermarkt entsprechend umgeordnet. Das Display zeigt die günstigste Route durch die Verkaufsregale an. Legt der Kunde ein Produkt in die Nähe des RFID-Lesers, wird dieses von der Einkaufsliste gestrichen.

[239] S. näher Coroama u.a. 2003, 11 ff.; Roßnagel/Müller, CR 2004, 626f.; Roßnagel 2004, 341f.; Siemoneit, in: NEXUS 2005, 203 ff.; Hansen/Fabian/Möller/Spiekermann, in: TAUCIS 2006, 143 ff.; Mattern 2005a, 24

[240] S. hierzu Müller, DuD 2004, 215 ff.

Interessiert sich der Kunde für zusätzliche Produktinformationen, kann er auf dem Display Gebrauchshinweise, Unverträglichkeiten oder Rezepte und Hinweise auf weitere zu diesem Produkt passende andere Produkte zur Kenntnis nehmen. Legt er zwei vergleichbare Produkte in den Warenkorb, erscheint auf dem Display eine Vergleichstabelle der wichtigsten Merkmale und eine Empfehlung entsprechend der bekannten Präferenzen des Kunden. Will der Kunde ein weiteres Produkt suchen, kann ihn der Einkaufswagen direkt dorthin führen, ohne dass er lange durch das Labyrinth der Regalreihen irren muss. Schließlich kann ihm auf dem Display angezeigt werden, wie hoch der Gesamtpreis der im Einkaufswagen jeweils enthaltenen Waren ist.

Beim Vorbeigehen an den Regalreihen erscheinen im Display des Einkaufswagens Werbebotschaften, die sowohl zu seiner Einkaufsliste, zu bereits gekauften Waren und zu den Waren passen, die der Kunde gerade passiert. Dabei wird er auch auf Sonderangebote, mögliche Rabatte und ähnliche Vergünstigungen hingewiesen. Falls das Informationssystem den Kunden identifiziert hat, entsprechen die Werbebotschaften seinen Kaufgewohnheiten, die das System aus seinen früheren Käufen abgeleitet hat.

Ein RFID-Leser im Regal kontrolliert den Warenbestand und übermittelt Änderungen an das Warenwirtschaftssystem des Supermarkts. Dadurch können Nachbestellungen automatisch angestoßen werden. Außerdem erhält das System für jede Produktgruppe eine aktuelle Anzeige der Verkaufszahlen. Stellen Kunden das Produkt nach Lesen der Produktinformationen wieder ins Regal zurück, werden auch diese Vorgänge dem System angezeigt. Die Preisanzeige kann abhängig vom Kaufinteresse oder Verfallsdatum dynamisch den Preis verändern. Hierfür kann sie auch die Treue des Kunden zu diesem Markt oder die bereits mit ihm erzielten Gesamtumsätze berücksichtigen.

Zum Bezahlen fährt der Kunde mit dem Einkaufswagen durch eine spezielle Schleuse. Sowohl diese als auch der Einkaufswagen lesen die Produktkennzeichen der darin befindlichen Pro-

dukte, um sicher zu gehen, dass alle Produkte erfasst werden.[241] Der Gesamtpreis wird unmittelbar von der Kreditkarte des Kunden abgebucht. Musste er diese beim Betreten des Ladens in das Lesegerät des Einkaufswagens stecken, gibt es kaum noch Möglichkeiten für Ladendiebstähle. Durch dieses Verfahren können der Kassenbereich und damit auch das Warten an der Kasse entfallen.

Wer keine Zeit hat, um im Supermarkt einzukaufen, kann dies auch von zu Hause aus erledigen.[242] Ein in die Tür des Kühlschranks eingelassener Touchscreen dient als Fenster in die große weite Einkaufswelt. Der Kühlschrank erkennt automatisch den Bedarf (fehlende Produkte, Produkte mit abgelaufenem Haltbarkeitsdatum) und generiert einen Vorschlag für eine Einkaufsliste. Will man ein bestimmtes Rezept kochen und gibt dies auf dem Touchscreen ein, wird die Einkaufsliste um die fehlenden Zutaten ergänzt. Wird die Einkaufsliste am Morgen vor der Arbeit abgeschickt, kann man am Abend auf den Rückweg die gefüllte Einkaufstüte in einem Abhol-Center in der Nachbarschaft abholen.

1.4.3 Fabrik

Um sich voll auf die jeweilige Tätigkeit konzentrieren zu können und die Hände für sie frei zu haben, wird der künftige Fabrikarbeiter durch Wearable Computing unterstützt werden.[243] Sein »Blaumann« ist aus High-Tech-Fasern gefertigt, die aus Gründen des Arbeitsschutzes bis zu 200 Grad hitzeresistent und extrem widerstandsfähig gegen mechanischen Abrieb sind. Im Arm des Anzugs ist ein kleines Display mit ein paar Tasten eingelassen. Dieser kleine »PC« ermöglicht, jederzeit drahtlos auf das globale

[241] Das schlichte Scannen aller Produkte am Ausgang des Markts ist gegenwärtig noch nicht möglich, hierfür müssen erst noch einige technische Probleme gelöst werden – s. z.B. Langheinrich 2007, 134.

[242] S. z.B. ISTAG 2001, 6; Siemoneit, in: NEXUS 2005, 208, 219.

[243] S. zu diesem Szenario Siemoneit, in: NEXUS 2005, 113 ff.

betriebliche Informationssystem zuzugreifen und mit Kollegen zu kommunizieren. Auf gefahrgeneigten Arbeitsplätzen überwachen die in den »Blaumännern« integrierten Sensoren die Körperfunktionen und leiten in einem Notfall wichtige Angaben über den Gesundheitszustand sofort an die Ambulanz weiter. Ergänzt wird diese Ausstattung durch einen kleinen Kopfhörer und eine Schutzbrille, auf der Informationen eingeblendet werden können, die den Eindruck erwecken, als ob sie die wahrgenommene Realität überlagern. In diesen Anzug wird die Identitätskarte eingesteckt, die ermöglicht, den jeweiligen Arbeiter über das fabrikweite Sensornetz zu orten, seine Zugangsberechtigung zu gewissen Fabrikbereichen zu überprüfen, ihm Werkzeuge und Vorrichtungen eindeutig zuzuordnen und seine Autorisierung zu kontrollieren, Maschinen nur entsprechend seinem Qualifizierungsprofil bedienen zu dürfen.

Beim Betreten der Fertigungshalle macht ein Piepton im Köpfhörer den Arbeiter darauf aufmerksam, dass er eine ortsgebundene Nachricht erhalten hat. Das Display an seinem Arm zeigt ihm seinen Arbeitsplan für heute. Die Durchführung der individuellen Bearbeitungsaufträge gestaltet sich inzwischen sehr einfach. Statt der früheren Zettelwirtschaft bringt heute jedes zu bearbeitende Werkstück seine Informationen elektronisch mit. Dank dieser eindeutigen Kennnummer und weiteren aus dem betrieblichen Informationssystem angeforderten Informationen ist die Bearbeitung heute ein Kinderspiel. In die Schutzbrille werden die nächsten Bearbeitungsschritte entsprechend eingeblendet und sind neben dem realen Werkstück zu sehen. Fertigungsfehler kommen heute fast nicht mehr vor.

Bearbeitete Werkstücke und verbrauchte Werkzeuge werden in spezielle Behälter gelegt, Reststoffe automatisch eingesammelt. Sie werden automatisch von mobilen Robotern abgeholt, zum nächsten Bearbeitungsschritt, zur Entsorgung oder zur Instandsetzung gebracht. Die Roboter bringen auch immer rechtzeitig neue Werkstücke und Werkzeuge sowie sonstiges Material. Produktionsstillstände kommen kaum noch vor. Die

umfassende Ausstattung der stationären Maschinen und der mobilen Betriebsmittel mit Sensoren und der Einsatz von Robotik ermöglichen eine hohe Transparenz über Ort und Zustand der Werkzeuge und Vorrichtungen sowie den aktuellen Stand der Produktion. Da die Werkstücke ihren Bearbeitungsplan »mit sich tragen«, kann Verantwortung an die dezentralen betriebsinternen Logistikeinheiten delegiert werden. Das virtuelle Gedächtnis jedes Werkstücks »weiß«, welche Bearbeitungsschritte das Werkstück schon erfahren hat und welche weiteren Schritte in welcher Reihenfolge und an welchen Orten noch erforderlich sind. Durch Kommunikation mit den Werkzeugmaschinen und den Robotern können sie ihren Weitertransport jeweils selbst organisieren. Auf diese Weise können sich die kleineren Logistikeinheiten selbst koordinieren und selbsttätig entscheiden, wie auf kleinere Ausfälle und Unregelmäßigkeiten reagiert wird.

Treten doch größere Probleme auf, können der für die Produktionslinie Verantwortliche oder der zuständige Reparaturmeister schnell gefunden werden. Der betroffene Arbeiter stellt mit einigen Sprachkommandos und dem Armdisplay eine Anfrage an das betriebliche Informationssystem, wo sie sich befinden, und baut zu ihnen eine Sprachverbindung auf. Muss er sie suchen, schaltet er das Display auf Navigationsmodus. Merkt das System, dass er sich in Eile befindet und nicht mehr auf die Fabrikkarte auf dem Armdisplay schaut, blendet es ihm die entsprechenden Richtungspfeile in die Brille ein.

Jeder Reparaturarbeiter hat die ihm zugeordneten Werkzeuge in seinem Werkzeugkoffer, den er morgens aus seinem Spind mitbringt und am Ende der Arbeit dort auch wieder deponiert. Hat er beim Einräumen des Werkzeugs eines vergessen, meldet ihm der Koffer, welches Werkzeug fehlt. Wenn er sich nicht mehr daran erinnert, wo er es verlegt hat, kann er es über das Sensornetzwerk und die RFID-Leser suchen lassen. Benötigt er für einen Auftrag eine zusätzliche Vorrichtung oder ein Spezialwerkzeug, kann er ebenfalls durch ein paar Tastendrucke auf dem Armdisplay herausfinden, wo es sich gerade befindet und ob es zurzeit

von einem Kollegen gebraucht wird. Viele lange Holwege kann man sich somit sparen, da der Aufenthaltsort und der Status der Werkzeuge dem System bekannt ist.[244]

1.4.4 Studieren

Trotz aller Möglichkeiten des E-Learning bleiben die Vorlesungen und Seminare der entscheidende Bestandteil der Wissensvermittlung. Allerdings werden die Lehrveranstaltungen durch multimediale Angebote unterstützt. Im Hörsaal kann der Hochschullehrer durch Sprache oder Gesten gesteuert unterschiedliche Medien einsetzen. Diese werden – soweit dies didaktisch hilfreich ist – den Studierenden beim Betreten des Hörsaals auf ihre persönlichen Endgeräte übertragen. Am Ende jeder Veranstaltung bitten die Hochschullehrer um eine Rückmeldung der Studierenden. Hierfür hat sich als beliebteste Evaluationsmethode herausgestellt, dass die Studierenden beim Verlassen des Hörsaals eine an den Lehrenden gerichtete anonyme Kurzbotschaft hinterlassen. Dieser »sammelt« die virtuellen »Post-its« mit seinem persönlichen Endgerät ein und lässt sie von seinem virtuellen Assistenten auswerten.

In allen Universitäten herrscht Raumnot. Insbesondere fehlt es an Räumen, für die sich – wie bei Forschungsgruppen oder studentischen Arbeitsgruppen – der Bedarf relativ kurzfristig ergibt. Um eine optimierte Raumverteilung zu erreichen, erkennt das Raumbelegungssystem, welcher Raum von wie vielen Personen aktuell belegt ist. Auf diese Informationen können Berechtigte mobil zugreifen, damit sie einen freien Raum leicht für sich belegen können. Bei dieser Abfrage kann auch geklärt werden, ob der Raum geeignet ausgestattet ist. Weiterhin wird ein Dienst angeboten, der alle Teilnehmer des Treffens automatisch über den neuen Tagungsraum oder eine zeitliche Verlegung der Veranstaltung informiert. Sofern den Teilnehmern der neue Tagungsraum

[244] S. zu kritischen Aspekten dieses Szenarios Siemoneit, in: NEXUS 2005, 117 ff.

unbekannt ist, leitet sie ein Leitsystem mit Hilfe ihres Endgeräts zum neuen Veranstaltungsort – falls er an einem anderen Standort der Universität ist, unter Berücksichtigung aktueller Fahrpläne und freier Parkplätze. In Gebäuden kann man sich auch durch die elektronischen Türschilder unterstützen lassen, deren Angaben sich beim Vorbeigehen zu Richtungspfeilen verändern.

Die Universität bietet auf ihrem Gelände auch einen Personensuchdienst an, den Hochschulangehörige abonnieren können, in den aber auch Gäste sich einklinken können.[245] An diesem Dienst kann man aktiv und passiv teilnehmen. Als aktiver Teilnehmer kann man an den Dienst Anfragen stellen, wo sich eine bestimmte Person gerade befindet, oder um eine Benachrichtigung bitten, wenn ein bestimmtes Ereignis eintritt, etwa wenn ein Gast auf dem Universitätsgelände eintrifft, wenn sich ein Freund in einem Abstand von weniger als 200 m aufhält oder wenn sich eine Gruppe von Personen in einem bestimmten Raum trifft. Man kann aber auch nicht personenbezogene Hinweise anfordern, etwa wenn ein Lieblingsessen in der Mensa angeboten oder ein bestelltes, aber ausgeliehenes Buchs zurückgegeben wird. Als passiver Teilnehmer hat man die Möglichkeit, die Standortdaten für solche Zwecke für bestimmte Personen, Orte oder Ereignisse freizugeben oder zu sperren.

In der Universität können an allen Stellen virtuelle Nachrichten für bestimmte oder alle Personen hinterlassen werden. Ist eine Person gerade nicht in ihrem Zimmer oder an ihrem üblichen Lernplatz, kann man dort eine für sie bestimmte Nachricht zurücklassen, die nur sie mit ihrem persönlichen Endgerät lesen kann. Die elektronische Annonce, dass man ein Lehrbuch oder ein Notebook verkaufen will, wird an hoch frequentierten Plätzen hinterlassen. Jeder, der vorbeigeht und sich für Annoncen interessiert, kann sie lesen. Aus der Fülle der Annoncen wird der persönliche Assistentenagent diejenigen heraussuchen und präsentieren, die dem Interessensprofil oder sogar einer bekannten Suchabsicht des Nutzers entsprechen.

[245] S. hierzu Heesen, in: NEXUS 2005, 138 ff.; Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 57 ff.

Nachrichten können auch an bestimmte Räume adressiert werden. So kann zum Beispiel ein Student, der seine Handschuhe im Vorlesungssaal vergessen hat, es aber erst merkt, wenn der Raum schon wieder mit anderen Studierenden gefüllt ist, an alle in dem Raum Anwesenden die Bitte richten, unter ihrem Tisch zu schauen, ob dort die Handschuhe liegen. Als neue Übung ist derzeit gerade beliebt, an den Mensaeingängen Hinweise über die Qualität des Mensaessens zu hinterlassen. Wer die Mensa verlässt, postet anonym, was er gegessen und wie es ihm geschmeckt hat. Dadurch entsteht eine Hitparade der angebotenen Speisen, an dem sich die Nachkommenden orientieren, und insgesamt erhält die Mensaleitung dadurch eine tägliche Rückmeldung über die Zufriedenheit mit dem Angebot.

Auf der elektronischen Anzeigetafel vor jedem Hörsaal wird angezeigt, welche Lehrveranstaltung stattfindet. Wer wissen will, welcher Stoff gerade behandelt wird und wie der gesamte Inhalt der Veranstaltung gegliedert ist, kann mit seinem persönlichen Endgerät auf die Anzeigetafel zeigen und erhält diese Informationen präsentiert. Diese gleiche Technik wird genutzt zur Erläuterung von Exponaten und Demonstratoren von Forschungsergebnissen in den Hallen und Fluren der Universität. Interessierte erhalten durch »Anklicken« der Gegenstände weitere Informationen.

1.4.5 Neue Geschäftsmodelle

Wenn wertvolle Produkte mit Techniken der allgegenwärtigen Datenverarbeitung ausgestattet sind, wenn sie eine integrierte Informationsverarbeitung, eine eindeutige fernabfragbare elektronische Identität und Sensoren zur Wahrnehmung ihres Kontextes aufweisen, könnten sich vollkommen neue Geschäftsmodelle als attraktiv erweisen. Wer solche Geräte zu Eigentum erwirbt,

muss den gesamten Preis für das Gerät bezahlen, unabhängig davon, ob er es oft oder selten, intensiv oder zurückhaltend, über einen langen Zeitraum oder nur kurzfristig nutzt. Er ist für die Wartung und Instandhaltung des Geräts verantwortlich, muss sich um Ersatzteile und Reparaturen selbst kümmern und dies gesondert bezahlen. In diesem Fall hat der Vertragspartner ein Interesse an einer Lebensdauer des Geräts nur für die Dauer der Garantie und freut sich, wenn der Nutzer bald wieder ein neues kauft. Häufige Modellwechsel mit künstlicher Produktveralterung für das gekaufte Gerät sind die Folge. Kosten der Unterhaltung und Betriebsmittel berühren den Hersteller nicht – allenfalls als Verkaufsargument –, dafür aber den Eigentümer – etwa im Fall von Preissteigerungen für Treibstoff – umso mehr.

Sofern dem Käufer eines solchen Geräts vor allem an dessen Funktion – und weniger an dessen Statuswert – liegt, könnte es sich anbieten, dieses Gerät nur noch zu leasen oder zu leihen.[246] Die Bezahlung könnte nutzungsabhängig und nicht nur zeitabhängig erfolgen. Kunden zahlen nur für das, was sie tatsächlich nutzen, und nicht nur für die Möglichkeit der Nutzung.[247] Die tatsächliche Nutzung von Gegenständen zu ermitteln und an den Verleiher weiterzumelden oder für diesen zu speichern, könnten Techniken der allgegenwärtigen Datenverarbeitung übernehmen.[248] Übermäßige oder nicht vereinbarungsgemäße Nutzung könnten durch Techniken des Digital Rights Managements (DRM) unterbunden werden. Damit könnten alle genannten Nachteile für den Nutzer des Geräts vermieden werden. Aufwand und Kosten für Instandhaltung sowie die Risiken des Verlusts oder der Beschädigung müsste der Verleiher tragen. Der Nutzer müsste sich um nichts kümmern und würde nur den Wert bezahlen, den er tatsächlich durch Nutzung des Geräts »verbraucht«.

246 Dies wird nicht für alle Gegenstände attraktiv sein. Oft wird die durch Eigentum vermittelte Möglichkeit der unbegrenzten Nutzung bevorzugt.

247 S. z.B. Fleisch/Christ/Dierkes 2005, 25f.; Siemoneit, in: NEXUS 2005, 179, 215.

248 Mattern 2007a, 18f.; Sietmann, c't 2004/16, 89.

Erfolgt eine nutzungsabhängige Abrechnung (Pay-per-Use), muss festgestellt werden können, wie oft oder wie intensiv die Nutzung erfolgt.[249] Diese Daten müssen in verlässlicher und beweissicherer Weise erhoben und gespeichert werden. Ob sie in dem Gerät gespeichert und am Ende der Nutzungszeit mit dem Gerät zurückgegeben oder in gewissen Abständen an den Eigentümer übermittelt werden, hängt vom Gegenstand, der Weise seiner Nutzung, dem Abrechnungszeitraum und dem Risiko des Verlusts des Gegenstands und seiner Daten ab. Jedenfalls entsteht ein »Gedächtnis« des Gegenstands, mit dessen Hilfe die Nutzungsgeschichte nachgezeichnet und zur Grundlage der Abrechnung gemacht werden kann.

Neben einer nutzungsabhängigen Abrechnung kann auch eine risikoorientierte Abrechnung (Pay-per-Risk) erfolgen. So kann zum Beispiel eine Autovermietung ihren Preis nicht nur an den gefahrenen Kilometern orientieren, sondern auch an dem pfleglichen Umgang des Mieters mit dem Fahrzeug. In den USA erheben bestimmte Leihwagenunternehmen von ihren Kunden ein zusätzliches Entgelt für »gefährliches Fahren«, wenn das Auto schneller als 79 km/h fährt.[250] Ähnliche riskante Verhaltensweisen könnten auch bei anderen Gegenständen definiert und tarifiert sowie im Anschluss daran beim einzelnen Nutzer auch gemessen und gespeichert werden.

Die Orientierung am tatsächlichen Risiko bietet sich vor allem für Versicherungen an. Die Prämien könnten dann – je nach riskantem Verhalten – gerechter in Rechnung gestellt werden (Pay-as-You-Drive), weil die Gesamtheit der Schäden nicht mehr von allen Versicherten gleich, sondern entsprechend ihrem Risikobeitrag aufgebracht werden müssten. So könnten etwa Autoversicherungen ihre Prämien an den konkreten Risiken orientieren, indem bestimmte Parameter der Fahrbedingungen (Nacht, Regen, Eis und Schnee), des Fahrverhaltens (Geschwindigkeit, Auffahr-

249 S. Mattern 2003c, 23; Mattern 2005a, 15.

250 Mattern 2003c, 34.

dichte, Beschleunigung) und der Orte des Parkens (Diebstahls- oder Beschädigungsrisiko) aufgezeichnet und in regelmäßigen Abständen an die Versicherung geschickt werden. Dem Fahrer könnte die Prämiengruppe, in die eine Fahrt fällt, im Armaturenbrett angezeigt werden.[251] Im Schadensfall könnten die aufgezeichneten Daten auch bei der Klärung der Schuldfrage helfen.[252] In Feldversuchen wurden am Fahrverhalten orientierte Autoversicherungen bereits mehrfach getestet.[253] Erste Angebote solcher Versicherungen sind bereits auf dem Markt.[254] Auf Testmärkten waren viele befragte Autofahrer bereit, für eine 25-prozentige Reduktion des Tarifs im Rahmen einer dynamischen Autoversicherung die Versicherung wissen zu lassen, wo man sich mit dem Auto befindet.[255]

[251] S. z.B. Coroama/Langheinrich 2005; Coroama/Langheinrich 2006; Mattern 2004, 327; Mattern 2005a, 15; Mattern 2007a, 18; Hansen/Fabian/Klafft, in: TAUCIS 2006, 46; Siemoneit, in: NEXUS 2005, 179, 215.

[252] Mattern 2003c, 34.

[253] 2007 von der WGV-Versicherung zusammen mit T-Systems mit 1500 Fahranfängern; 2004 bis 2006 in Dänemark mit 300 Fahrern – Welt kompakt vom 15.3.2007, 11.

[254] Britische Versicherungsgesellschaft Norwich Union – Welt kompakt vom 15.3.2007, 11.

[255] Mattern 2004, 327.

2. DATENSCHUTZRISIKEN

Wird versucht, die Visionen allgegenwärtiger Datenverarbeitung umzusetzen, und werden die im vorangegangenen Abschnitt beschriebenen Anwendungen realisiert, werden durch die Verarbeitung personenbezogener Daten vielfältige Risiken für die informationelle Selbstbestimmung, für die Entscheidungsfreiheit, für die Entfaltungsfreiheit, für die Ausübung vieler anderer Grundrechte und für die demokratische Ordnung entstehen.

2.1 Allgegenwärtige Datenerhebung

Anwendungen der allgegenwärtigen Datenverarbeitung werden künftig in unmerklicher und vielfach undurchschaubarer Weise nahezu überall und immer automatisiert personenbezogene Daten in einem sehr großen Umfang und mit hoher Aussagekraft erheben und weitergeben, damit sie für vielfältigste Zwecke genutzt werden können.

2.1.1 Unbemerkte Datenerhebung

Ein wesentliches Ziel von Ubiquitous Computing ist es, die Datenverarbeitung in den Hintergrund treten zu lassen, den Nutzer von Datenein- und ausgaben zu entlasten und ihm die gewünschten Funktionen selbsttätig zu bieten oder anzubieten. Daher ist es ein Wesensmerkmal allgegenwärtiger Datenverarbeitung, dass sie vom Nutzer unbemerkt erfolgt. Identifikatoren, Lokalisatoren, Kameras, Mikrophone oder sonstige Sensoren sind daher in die Gegenstände integriert.[1] RFID-Tags werden durch drahtlose

[1] Müller/Handy, DuD 2004, 656; Langheinrich 2007a, 130.

Kommunikation unbemerkt ausgelesen,[2] Sensoren nehmen Daten aus der Umwelt lautlos und unsichtbar auf, die Ortsbestimmung erfolgt durch die Gegenstände unerkannt.[3] Techniken des Wearable Computing nehmen unbemerkt Menschen auf, denen ihre Träger begegnen. Dadurch bleibt nicht nur die allgegenwärtige Erhebung personenbezogener Daten für den Betroffenen unbemerkt, sondern wird – noch weitergehender – zu einem selbstverständlichen, nicht mehr wahrnehmbaren Teil seines Lebens.

Wird der Einzelne durch die Datenverarbeitung in seiner Umgebung und in den von ihm genutzten Alltagsgegenständen allgegenwärtig begleitet, wird sie unmerklich in sein Verhalten und sein Handeln integriert. Wenn zum Beispiel ein »mitdenkendes« Einkaufsregal Position und Art der eingeräumten Ware über RFID-Leser festzustellen vermag, dann wird der Datenverarbeitungsvorgang Bestandteil des Herausnehmens und Zurücklegens der Ware. Nehmen sehr kleine, in die Umwelt integrierte Sensoren ihre Umwelt wahr und wird dadurch in dem angeschlossenen Informationssystem die reale Welt in der virtuellen Welt abgebildet, so wird dabei – gewollt oder notgedrungen – auch der einzelne Mensch, der sich in dieser Umwelt bewegt, mit aufgenommen und ist bereits deshalb schon – unbemerkt – Gegenstand der datenerhebenden und -verarbeitenden Vorgänge.[4]

Im Ergebnis ist die Datenerhebung für die Betroffenen in der Regel intransparent. Kein Betroffener wird erkennen, dass Daten über ihn erhoben werden. Kein Betroffener wird mehr im Voraus wissen können, wer welche Daten durch die ihn umgebenden Gegenständen erhebt, nutzt und in anderen Zusammenhängen für oder gegen ihn verwendet.[5] Die Ahnung aber, dass jedes Verhalten irgendwo und irgendwie registriert werden könnte, wird zu Verhaltensanpassungen führen.

[2] Einfache Tags nach dem EPCglobal Standard haben keinen Zugriffsschutz – s. Fabian, in: TAUCIS 2006, 263; AK Technik 2006, 4, 7; s. auch Voort/Ligtvoet 2006, 18; UNESCO 2007, 49.

[3] S. z.B. Sietmann, c't 2004/16, 87f.; UNESCO 2007, 53.

[4] Roßnagel/Müller, CR 2004, 627; Müller/Handy, DuD 2004, 656; AK Technik 2006, 22.

[5] Roßnagel/Pfitzmann/Garstka 2001, 23.

2.1.2 Automatische Datenerhebung

Die Datenerhebung erfolgt automatisch. Die Arbeitsentlastung und Kostensenkung durch allgegenwärtige Datenverarbeitung soll gerade in der Weise erfolgen, dass sich der Nutzer nicht mehr um die Erhebung der erforderlichen Daten kümmern muss. Sensoren erheben die Kontextdaten ohne besonderen Befehl – permanent oder bei bestimmten Ereignissen. Neue Ortsbestimmungen erfolgen bei jeder Bewegung automatisch. Sensornetze registrieren über ganze Bereiche hinweg jede relevante Veränderung. Tracking-Systeme verfolgen die Bewegung von Gegenständen und Menschen selbsttätig. Gegenstände werden von RFID-Systemen, Menschen von Zutrittskontrollsystemen ohne besonderes Zutun erkannt und identifiziert.[6]

Durch die durchgängige Automatisierung verändert sich die Art der Datenerhebung – mit entscheidenden Veränderungen hinsichtlich der Wahrnehmung und der Handlungschancen des Betroffenen. Manuelle und auch die bisherige automatisierte Datenerhebung ermöglicht ein Wahrnehmen und Erinnern und bietet Chancen, durch das eigene Verhalten in Voraus oder im Nachhinein darauf zu reagieren. Die Datenerhebung erfolgt entweder unter Mitwirkung des Betroffenen oder zumindest durch besondere Handlungen, die er von anderen Handlungsvollzügen deutlich abgrenzen kann. Er weiß, dass bei Telefonaten die Zeit und die Teilnehmer gespeichert werden, er ist sich darüber bewusst, dass das Surfen im Internet Datenspuren beim Provider und den besuchten Seiten hinterlässt, und er ist darüber informiert, dass die Kreditkartenunternehmen seine mit der Kreditkarte durchgeführten Einkäufe verarbeiten. Die Erhebung von

[6] Zur ständigen Beobachtung s. auch SWAMI 2006c, 8; Artikel-29-Datenschutzgruppe 2005a, 6

Daten ist an besondere Momente und Anlässe geknüpft. Diese kennt der Betroffene im Voraus und kann sie – beschränkt – vermeiden. An sie kann er sich – grundsätzlich – erinnern oder er kann sie im Nachhinein noch rekonstruieren. Er hat dadurch zumindest noch eine Chance zu wissen, was sein Kommunikationspartner über ihn wissen kann.

Doch diese ausgezeichneten Anlässe und Momente der Datenerhebung verschwinden in gleichem Maß, wie die Computer selbst verschwinden und allgegenwärtig werden. Die durchgängige automatisierte Datenerhebung potenziell jeder Handlung verhindert es, sich an sie zu erinnern oder sie zu rekonstruieren. Selbst wenn man sich solcherlei Datensammlungen entziehen möchte, wird dies in Zukunft aufgrund des mangelnden Bewusstseins über die Momente dieser Erhebungen kaum noch möglich sein.[7] Damit entfällt auch die Chance eines Betroffenen, das Wissen eines Kommunikationspartners über ihn selbst abzuschätzen.

2.1.3 Umfangreiche Datenerhebung

Die Datenerhebung wird in ihrem Umfang exorbitant zunehmen. Zum einen wird die Zahl der datenverarbeitenden Systeme extrem ansteigen. Der massenhafte Einsatz von datenverarbeitenden Gegenständen vervielfacht die Vorgänge der Erhebung und Verarbeitung personenbezogener Daten erheblich. In ihrer Fülle und Komplexität sind sie durch den Einzelnen kaum mehr zu überschauen.[8]

Zum anderen wird die Zahl der benötigten Daten – auch personenbezogener Daten – pro Informationssystem ansteigen. Alle Anwendungen der allgegenwärtigen Datenverarbeitung zielen auf die Erhebung und Verarbeitung von Daten aus der realen Welt oder benötigen diese Daten, um ihre Funktionen erfüllen zu können. Identifikations-, Tracking-, Lokalisations-, Monitoring-,

[7] S. Langheinrich 2005a, 336.

[8] S. Mattern 2003c, 31; Roßnagel/Müller, CR 2004, 628; UNESCO 2007, 46.

Steuerungs- und Entscheidungssysteme benötigen eine gewaltige Menge von Umgebungsdaten. Vielfach werden diese Systeme eingesetzt, weil sie ermöglichen, Daten zu erheben, die bisher nicht erhoben werden konnten, weil dies zu schwierig oder zu aufwändig war.

Bei vielen Anwendungen allgegenwärtiger Datenverarbeitung wird versucht, angepasste Reaktionen der Technik dadurch zu erreichen, dass man statt auf künstliche »Intelligenz« auf eine möglichst exakte Erfassung des aktuellen Kontextes setzt.[9] Kennt etwa ein Gegenstand seinen Aufenthaltsort und kann er in seiner Umgebung weitere Gegenstände und Menschen identifizieren, kann er eventuell auch ohne echtes Verständnis der Situation sinnvoll auf diese reagieren. Oder man versucht, durch hohe Redundanz, auch in der Datenerhebung, technische Unzuverlässigkeiten – beim Lesen von RFID-Tags, bei der Ortsbestimmung, bei der Kontexterfassung – auszugleichen. Für diese Redundanz kommt es auf das Sammeln von möglichst vielen Daten an, da bei ihrer Auswertung zur Situationseinschätzung – sofort oder später – grundsätzlich alles relevant sein kann. Dies erhöht den Sammeleifer: Selbst scheinbar banale Daten können durch Computeranalyse mit relevanten Fakten korreliert werden.[10]

Da die Daten automatisiert erhoben werden und die Verfügbarkeit von Speicherplatz in der Regel keine Beschränkung darstellt, gibt es kaum innere Begrenzungen für den Umfang der zu erhebenden Daten.

2.1.4 Ständige und ubiquitäre Datenerhebung

Die Erhebung der Daten wird eine neue Ausdehnung erfahren. Sie wird zeitlich vielfach rund um die Uhr stattfinden und örtlich nahezu unbegrenzt erfolgen. Sie wird damit in zeitlicher und in

[9] S. oben 39 ff. sowie Langheinrich 2005a, 337; zur Redundanz der Datenerhebung s. auch BMBF 2007, 22.

[10] S. Langheinrich 2005a, 337.

räumlicher Hinsicht grenzenlos sein. Betroffene müssen immer und überall damit rechnen, dass personenbezogene Daten von der sie umgebenden gegenständlichen Welt erhoben werden.

Kommunikationsfähige Gegenstände und Sensornetze sind fast immer aktiv, beobachten ihre Umwelt permanent und sammeln eine Unmenge von Daten, um den Nutzern jederzeit ihre Dienste anbieten zu können und sie über alle erfolgten Ereignisse zu informieren. Ähnlich wie der PC die »Online-History« der besuchten Web-Seiten speichert, dürften die Gegenstände und die in der Umgebung verteilte allgegenwärtige Datenverarbeitung ihre jeweilige »Offline History« speichern.[11] Heizungs- und Klimaanlage speichern permanent relevante Umwelt- und Nutzungsdaten, Sicherheitssysteme kontrollieren alle sicherheitskritischen Bereiche, Trackingsysteme erheben die Aufenthaltsorte von Gegenständen und Menschen, Verkehrsassistenzsysteme verarbeiten beim Fahren alle relevanten Daten des Fahrerverhaltens, des Kraftfahrzeugzustands und der Verkehrsumwelt, virtuelle »Tagebücher der Sinne« oder Systeme wie »DejaView«[12] erheben alle oder ausgewählte Ereignisse, die ihrem Nutzer widerfahren. In einer stark entwickelten Welt allgegenwärtiger Datenverarbeitung könnten einem ständig viele Menschen begegnen, die mit Techniken des Wearable Computing ausgerüstet sind und Unmengen Daten über ihre Umgebung aufnehmen.

Die Datenerhebung wird überall erfolgen.[13] Der Vision des Ubiquitous Computing entsprechend sind irgendwann einmal fast alle Gegenstände mit Informationstechnik ausgestattet und der Fähigkeit versehen, ihre Umwelt wahrzunehmen. In dem Umfang, in dem allgegenwärtige Datenverarbeitung Wirklichkeit wird, nehmen die Verbreitung und die Dichte der Datenerhebung durch die umgebenden Gegenstände zu. Tendenziell wird dies alle Lebensbereiche umfassen. Datenerhebungsfreie Räume müssen dann durch besondere Maßnahmen geschaffen werden.

[11] S. hierzu näher Mattern 2003c, 31.

[12] S. zu diesen oben 70 f.

[13] Ebenso Langheinrich 2005, 336; Sietmann, c't 2004/16, 88.

Auch wenn die Datenerhebung in Kraftfahrzeugen oder in Gebäuden zwar sehr umfassend ist, kann sie doch weitgehend auf diese spezifischen Bereiche hochintensiver Datenerhebung begrenzt werden. Bewegt sich das Kraftfahrzeug, gehen aber auch die Kontrollmöglichkeiten durch Verkehrstelematik weit über ein Mautsystem hinaus – nicht nur bestimmte Stationen auf Autobahnen und am Rande von Stadtkernen nehmen Daten auf. Vielmehr werden Daten durch die Kommunikation mit dem Auto und dessen Ortsbestimmung ständig und überall erhoben. Noch viel weitergehender ist die Erfassung durch andere Systeme der allgegenwärtigen Datenverarbeitung. Beispielsweise gehört es zur Bestimmung von Sensornetzen, dass sie in dem Bereich, in dem sie ausgebracht sind, lückenlos funktionieren und alle Veränderungen registrieren. Ebenso ist es das Ziel von Lokalisationssystemen, überall zu funktionieren und die Ortsdaten eines Gegenstands oder Menschen zu bestimmen, egal wo dieser sich aufhält. Trägern von Erhebungsinstrumenten, die in die Kleidung integriert sind, kann man überall begegnen.

2.1.5 Erhöhte Aussagekraft der erhobenen Daten

Die durch Systeme der allgegenwärtigen Datenverarbeitung erhobenen Daten werden neue Qualitäten haben, die vor allem in der inhaltlichen und zeitliche Nähe zum realen Geschehen sowie in der Dichte der Angaben liegen und die damit eine viel höhere Aussagekraft erlangen können als bisher erhobene Daten.

Seit es automatisierte Datenverarbeitung gibt, haben sich die erhobenen Datensätze kaum verändert: Durch manuelle Datenerhebung werden Name, Adresse, Alter und weitere Identifikationsdaten erhoben. Durch automatisierte Auswertungen werden weitere Daten gesammelt wie das Kaufverhalten, das Verhalten am Telefon oder im Internet. Daraus können weitergehende

Schlussfolgerungen gezogen und Profile über die Betroffenen erstellt werden.[14]

Mit Ubiquitous Computing eröffnet sich nun eine völlig neue Art der »Echtzeit«-Daten – der momentane Aufenthaltsort, der aktuelle Gesundheitszustand, oder die tatsächlichen (im Gegensatz zu den von uns vorgegebenen) Vorlieben.[15] Diese Daten werden nicht über Angaben des Betroffenen oder aus Datenspuren in automatisierten Systemen abgeleitet, sondern durch direkte Messung der Umwelt und des tatsächlichen Verhaltens des Betroffenen gewonnen. Solche Daten waren bisher nur als Momentaufnahmen – zum Beispiel bei einem Arztbesuch – möglich. Durch Ubiquitous Computing können sie permanent und in Echtzeit aufgenommen werden. In dieser detaillierten Form und in diesem Umfang waren sie bisher niemals zuvor ermittelbar.[16]

Die Realitätsnähe, der Umfang und die Dichte der Daten erlauben auch sicherere Schlussfolgerungen. Wenn etwa über Wearable Computing bestimmte Situationen in Bild und Ton protokolliert worden sind, ist dies erheblich aussagekräftiger als die oft schwache Erinnerung eines Zeugen. Wenn das »Gedächtnis« der Dinge genutzt werden kann, in dem alles protokolliert ist, was diese Dinge aufgenommen haben, kann dies – insbesondere bei Übereinstimmung unterschiedlicher Protokolle – zu vertrauenswürdigen Ergebnissen führen. Werden über eine Person die ständig und überall aufgenommenen Daten ausgewertet, erlaubt dies erheblich intensivere Einblicke in ihr Verhalten, ihre Beziehungen und ihre Persönlichkeit als bisherige Datensammlungen.

Eine besondere Bedeutung dürfte dabei den Sammlungen von Ortsdaten zukommen. Denn wissen Dinge, wo sie sind oder wo sie waren, dann kann damit leicht auf den Aufenthaltsort einer Person geschlossen werden, wenn die persönlichen Gegenstände dies verraten.[17] Nimmt man mehrere Ortsdaten zusammen, können auch Tagesabläufe oder Beziehungsnetzwerke erfasst werden.[18]

Zwar kann für Orts- und Sensordaten ebenso wie für Produktkennungen, die auf RFID-Tags gespeichert sind, für sich genommen der Personenbezug fehlen,[19] dieser wird aber vielfach mühelos durch eine Auswertung des Auslesekontextes oder weiterer Daten, etwa über das Zahlungsmittel, die Kundenkarte oder die körperliche Nähe hergestellt.[20] Sie sind daher in der Regel als personenbeziehbar einzustufen.

Daher können Sensor- oder RFID-Systeme zu vielfältigen Erhebungen personenbezogener Daten genutzt werden. Eine verbesserte Identifizierung einzelner Gegenstände erhöht gleichfalls die Möglichkeiten zur eindeutigen Identifikation der einen Gegenstand mitführenden Person und die informationelle Verfolgung dieser Person über die Verfolgung des Gegenstands. Dies ist besonders kritisch beim Einsatz solcher Techniken in Gesundheits-, Sicherheits- und Zahlungssystemen, bei denen personenbezogene Daten eng mit einem RFID-Tag verknüpft oder direkt darauf gespeichert sind.[21]

Nimmt man mehrere Datenquellen der allgegenwärtigen Datenverarbeitung zusammen ergeben sich dichte Angaben über das Verhalten einer Person. So können zum Beispiel aus Fahrerassistenzsystemen, die mit Systemen der Verkehrstelematik gekop-

14 S. Roßnagel/Banzhaf/Grimm 2003, 44 ff.

15 S. Langheinrich 2005a, 336.

16 S. Roßnagel/Müller, CR 2004, 628, Langheinrich 2005a, 336.

17 S. z.B. Müller/Handy, DuD 2004, 656; Mattern 2007a, 21, der besondere Probleme für die »location privacy« sieht. S. hierzu auch die Große Anfrage der FDP-Fraktion vom Mai 2004, BT-Drs. 15/3256, und die Antwort der Bundesregierung vom Januar 2005, BT-Drs. 15/4725.

18 S. z.B. Heesen, in: NEXUS 2005, 142; Müller/Handy, DuD 2004, 656f.

19 S. z.B. Holznagel/Bonnekoh 2006, 21 ff.; Huber, MMR 2006, 733; Westerholt/Döring, CR 2004, 711; Artikel-29-Datenschutzgruppe 2005a, 9.

20 S. Möller/Bizer, in: TAUCIS 2006, 208; Müller/Handy, DuD 2004, 656; Artikel-29-Datenschutzgruppe 2005a, 9; AK Technik 2006, 8.

21 S. hierzu z.B. auch Langheinrich 2007a, 130; Müller/Handy, DuD 2004, 656; AK Technik 2006, 8 ff.; Artikel-29-Datenschutzgruppe 2005a, 6; Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2006, 193; UNESCO 2007, 47.

pelt sind, sehr aussagekräftige Informationen gewonnen werden – etwa über Kommunikationsvorgänge, über Bewegungsmuster, über den Tagesablauf, über das Fahrverhalten oder über Lenk- und Bremsvorgänge. Diese Daten können bei Kontrollen oder Unfällen – ungewollt – wie die Daten eines Fahrten- oder Unfallschreibers genutzt werden.[22]

Für fast alle Anwendungen der allgegenwärtigen Datenverarbeitung, die dem Nutzer angepasste Dienstleistungen bieten sollen, ist es erforderlich, dass die Anwendungen personenbezogene Daten über seine Interessen, Präferenzen, Bedürfnisse und aktuellen Situationen verarbeiten. Diese sehr aussagekräftigen Daten müssen von den Systemen entweder durch Beobachtung des Nutzers selbst gewonnen werden oder von ihm eingegeben werden. Alle diese Anwendungen arbeiten daher mit mehr oder weniger ausführlichen Nutzerprofilen.[23]

Hinsichtlich der Datenerhebung kann damit zusammenfassend festgehalten werden, dass Anwendungen der allgegenwärtigen Datenverarbeitung grundsätzlich eine Form der Alltagsüberwachung ermöglichen, die inhaltlich, zeitlich und räumlich weit über die heute mögliche automatisierte Informationsgewinnung aus Kreditkartentransaktionen, Telefonverbindungen und Internet-Nutzung hinaus geht.[24]

2.2 Allgegenwärtige Datenweitergabe und -nutzung

Sind die personenbezogenen oder personenbeziehbaren Daten in Systemen der allgegenwärtigen Datenverarbeitung erhoben, werden sie in der Regel für den jeweiligen Zweck des Systems ausgewertet. Oft ist hierfür ein Austausch der Daten zwischen unterschiedlichen Systemen sowie eine Profilierung des Nutzers erforderlich. Beides hat zusätzliche Datenschutzrisiken zur Folge.

[22] S. hierzu auch Roßnagel, NVZ 2006, 284f.; BSI 2006, 86, 89f.
[23] S. Roßnagel 2006, 152f.; Jandt/Laue, K&R 2006, 316 ff.
[24] S. Langheinrich 2005a, 336f.

2.2.1 Datenverbreitung

Alle Anwendungen allgegenwärtiger Datenverarbeitung setzen eine hochgradige kommunikative Vernetzung und einen intensiven kommunikativen Austausch von Daten voraus. Um ihre Funktion zu erfüllen, kooperieren sie über unterschiedliche Netzwerke mit anderen kommunikationsfähigen Gegenständen sowie sonstigen Sensor-, Identifikations- und Lokationssystemen sowie mit sonstigen Datenquellen im weltweiten Netz. Um ihre Funktion erfüllen zu können, nutzer- und situationsgerechte Dienstleistungen zu erbringen, greifen sie in der Regel auf den gesamten ihnen zur Verfügung stehenden Datenpool zurück. Dieser besteht sowohl aus zentral gespeicherten Daten als auch aus weit verzweigten dezentralen Datensammlungen anderer Anwendungssysteme. Jedenfalls werden die Ubiquitous Computing-Anwendungen nahezu immer eine Weitergabe von personenbezogenen Daten erfordern, um ihre Dienstleistung erbringen zu können. Hinzu kommt, dass viele an den Daten Interessierte versuchen werden, die interessanten Daten über Datenverbünde zusammenzuführen.[25]

Die notwendige Interkonnektivität zwischen vielen kommunikationsfähigen Gegenständen dürfte ein kaum mehr zu überblickendes Datennetz nach dem Motto schaffen: »Everything will be connected to everything else«. Dessen Datenströme sind mit traditionellen Zugriffskontrollen nicht mehr zu verwalten.[26]

Die dezentral gesteuerte – teilweise sogar spontane – Vernetzung und die – teilweise selbst organisierte – Kommunikation dieser Anwendungen untereinander führen zu einer Proliferation der erhobenen und verarbeiteten Daten. Niemand wird mehr im Voraus wissen können oder im Nachhinein rekonstruieren können,

[25] S. zu den Möglichkeiten unbemerkter Datenverbünde im Internet z.B. Roßnagel/Banzhaf/Grimm 2003, 79 ff.
[26] Langheinrich 2005a, 337.

welche Daten von den vielen kommunikationsfähigen Gegenständen erhoben und zwischen ihnen kommuniziert werden.[27]

2.2.2 Profilbildung

Vielfach setzen Anwendungen allgegenwärtiger Datenverarbeitung für ihre nutzergerechte Funktionserfüllung Profile der Nutzer über ihre Lebensumstände, Bedürfnisse und Präferenzen voraus.[28] Diese werden oft von den Nutzern selbst den Systemen anvertraut. Um die Dienstleistung situationsgerecht erbringen zu können, ist die ständig wiederholte Erhebung von Lebenssituationen des Nutzers erforderlich. Aus der Zusammenführung dieser Daten können sehr aussagekräftige Profile erstellt und für vielfältige Zwecke ausgewertet werden.

Allgegenwärtige Datenverarbeitung eröffnet die Möglichkeit, von den Betroffenen sehr feingranulare Profile über ihre Handlungen und ihre Verhaltensweisen in der körperlichen Welt zu erzeugen. Gelingt es etwa beim Anwendungsbeispiel Einkaufen den Verkaufsläden – zum Beispiel über ihre Kundenkarten – die RFID-Daten mit der Identität des Kunden zu verknüpfen, könnten sie das Kaufverhalten jedes Kunden detailliert nachvollziehen und auswerten. Alle im Szenario Reisen genutzten Informationssysteme verarbeiten Informationen über Reiseziele oder andere Präferenzen sowie Informationen über Aufenthaltsorte. Diese Daten könnten problemlos zu minutiösen Bewegungsprofilen zusammengeführt werden.[29]

Beispielweise können unter der Annahme, dass Gegenstände mit RFID-Tags sich über längere Zeiträume im Besitz der gleichen Person befinden, durch wiederholtes Auslesen der Identifikationsnummern Bewegungsprofile erstellt werden. Dabei spielt es

[27] Roßnagel/Pfitzmann/Garstka 2001, 23.

[28] S. oben ##.

[29] S. Roßnagel/Müller, CR 2004, 628; AK Technik 2006, 7; Artikel-29-Datenschutzgruppe 2005a, 6f.; UNESCO 2007, 47.

keine Rolle, ob beim Auslesen ausschließlich Identifikationsnummern übertragen werden und alle anderen Daten ins Hintergrundsystem verlagert sind. Je mehr Tags im Verkehr sind, desto besser sind die Möglichkeiten des Trackings. Bei Verfolgung mehrerer Personen lassen sich auch Kontaktprofile erstellen.[30] Diese Möglichkeit wird dann »zu einer Bedrohung der Privatsphäre, wenn RFID-Systeme zu einem ubiquitären Bestandteil des Alltagslebens werden«.[31]

Werden – um ein anderes Beispiel zu nehmen – die Daten aus Location Based Services gesammelt und ausgewertet, können Interessenprofile, Bewegungsprofile und Kontaktprofile erstellt werden.[32] Bei vielfacher Nutzung eines Autos kann die Kombination mit anderen Diensten und Anwendungen vom und zum Fahrzeug zu sehr detaillierten Profilen über Umfang und Art der Fahrzeugnutzung, über Routen und Aufenthaltsorte führen. Dadurch dass die Dienste und Anwendungen beinahe »always on« sind, kann hierdurch ein vollständiger Überblick über das Fahrverhalten und Lebensgewohnheiten über lange Zeiträume entstehen.[33]

Alle diese aussagekräftigen Daten und Profile des Nutzers können auch für unerwünschte Zwecke genutzt werden. Denn die durch diese Kommunikationen entstehenden Daten könnten nicht nur zur Unterstützung der Nutzer genutzt werden, sondern auch für die Verfolgung anderer Interessen wie die von Produktherstellern und -verkäufern, Werbetreibenden, Arbeitgebern, Versicherungen oder Anbietern sonstiger Dienste, Auskunfteien oder staatlichen Überwachungsbehörden, aber auch des neugierigen

[30] BSI 2004, 47; Artikel-29-Datenschutzgruppe 2005a, 7. Dagegen hält die Antwort der Bundesregierung auf eine Anfrage der FDP-Fraktion aus dem Jahr 2004, BT-Drs. 15/3190, die heimliche Erstellung von Bewegungsprofilen durch RFID-Systeme nach dem gegenwärtigen Stand der Technik für praktisch ausgeschlossen – und sieht daher keinen ergänzenden datenschutzrechtlichen Regelungsbedarf.

[31] BSI 2004, 47

[32] S. z.B. Roßnagel/Jandt/Müller/Gutscher/Heesen, 2006, 57 ff.; Jandt/Laue, K&R 2006, 316 ff.

[33] S. z.B. Roßnagel, NVZ 2006, 284.

Nachbarn oder eines eifersüchtigen Liebhabers.[34] Sie könnten genutzt werden, um etwa Verkehrsdelikte schneller und einfacher zu verfolgen oder um Straftaten aufzuklären sowie um Verdächtige oder auch Nicht-Verdächtige zu überwachen. Die Erhebung und Nutzung der Daten stehen in einem vielschichtigen Netz von Interessen und es ist für die Betroffenen im Voraus nicht zuverlässig abzuschätzen, wofür die Daten letztlich verwendet werden.

Die Möglichkeit der Profilbildung und Überwachung steigt, wenn die Organisation der Datenverarbeitung oder die Abrechnung der Dienstleistungen zentral oder abgestimmt erfolgt. Dies wäre etwa der Fall, wenn Umgebungsinformationssysteme immer den Standort der eingebuchten Nutzer kennen und die Leistungen der die Nutzer umgebenden Artefakte verrechnen. Die Profilbildung und Überwachung wird erschwert, wenn die Datenverarbeitung sehr dezentral und spontan erfolgt. Dies kann bei vielen verschiedenen Komponenten, die Daten anfragen, bei denen Daten abgefragt werden und die Daten verwalten, relativ schwierig werden, wenn diese von unterschiedlichen Verantwortlichen betrieben werden.

2.3 Ausspähen von Daten

Die Dinge beobachten und speichern viel. Wenn sie oft oder längere Zeit mit ihren Besitzern zusammen sind, sagt ihr »Gedächtnis« auch viel über das Verhalten und die Verhältnisse des Besitzers aus. Wenn die kommunikationsfähigen Dinge diese Erkenntnisse »ausplaudern«, können viele aussagekräftige Daten über den Besitzer preisgegeben werden.[35]

[34] S. Mattern 2005a, 21.

[35] S. auch Mattern 2005b, 52.

Risiken, dass Daten ungewollt preisgegeben werden, können durch verdecktes Auslesen, unerlaubtes Abhören und durch Datenlecks entstehen.[36]

Verdecktes Auslesen gespeicherter Daten kann zum einen benutzt werden, um die Bewegungen einer Person zu verfolgen. Hierfür genügt es die Identifikationsnummer eines von ihr getragenen Gegenstands auszulesen. Zum anderen können weitere im Speicher eines Gegenstands gespeicherte Daten ohne das Wissen des Trägers ausgelesen werden, die beispielsweise Ort und Datum des Kaufs eines Produkts angeben.[37] Nachteilig kann das verdeckte Auslesen auch dann sein, wenn dadurch bestimmte Umstände offenbar werden, etwa die oft zitierten Beispiele der Unterwäschenmarke, der Inhalte von Einkaufstaschen und von Einrichtungsgegenständen in einer Wohnung. In vielen Fällen kommt es dabei gar nicht darauf an, die Identität einer Person in Erfahrung zu bringen – es reicht zu wissen, dass *diese* Person einen Schwangerschaftstest in der Apotheke gekauft hat oder dass in *diesem* Haus modernste Unterhaltungselektronik steht.[38]

Statt aktiv RFID-Tags auszulesen, können Angreifer auch die Kommunikation mit legitimen Lesegeräten abhören, meist aus größerer Entfernung als beim aktiven Auslesen. Das Risiko wächst mit der maximalen Lesedistanz des regulären Lesevorgangs. Bei Transpondern mit sehr kurzer Reichweite ist das Risiko gering.[39] Selbst wenn die Daten auf dem Tag oder bei der Übertragung verschlüsselt werden, so können untere Protokollschichten wie beispielsweise das Anti-Kollisionsprotokoll das Vorhandensein bestimmter RFID-Tags einem Angreifer offen legen.

Unabhängig von der verwendeten RFID-Technologie besteht bei vielen RFID-basierten Anwendungen das Risiko, dass mehr

[36] S. zum Folgenden vor allem Langheinrich 2007a, 133; Müller/Handy, DuD 2004, 655 ff.; Müller/Handy 2005, 1145 ff.

[37] S. auch BSI 2004, 46; Fabian, in: TAUCIS 2006, 263; AK Technik 2006, 4, 7; s. auch Voort/Ligtvoet 2006, 18; UNESCO 2007, 49.

[38] Langheinrich 2007a, 130.

[39] BSI 2004, 55.

Daten als nötig ausgelesen, auf dem Tag gespeichert oder mit ihm verlinkt werden. Dieses generelle Problem automatischer Datenverarbeitung wird durch den potentiell flächendeckenden Einsatz von RFID-Tags signifikant verschärft. Gerade auch die kommerziellen RFID-Systemen zugrunde liegende Informationsinfrastruktur ist in ihrer aktuellen Ausprägung anfällig für Einbruchsversuche und Datenlecks.[40]

2.4 Verhaltensbeeinflussungen

Die Daten, die von kommunikationsfähigen Gegenständen und Sensornetzen aufgenommen werden, vermögen bei einer Zusammenführung ein weitaus detaillierteres Bild über Interessen, Neigungen, Verhaltensweisen und die allgemeine Verfassung und auch über die Schwächen einer Person zu liefern als die bisherigen Erhebungen durch Fragebögen oder auch die Erfassung der Datenspuren im Internet. Wer Dienste zur Sinneserweiterung, zur Gedächtnisunterstützung, zur Arbeitsentlastung oder zur Erhöhung der Bequemlichkeit oder zur Verstärkung von Sicherheit nutzt, erzeugt durchaus ungewollt und quasi als Nebenprodukt individuelle Aktivitätsprotokolle, die beinahe lückenlos Auskunft über das Leben einer Person geben können.[41] Das Verhalten und die Präferenzen eines Menschen lassen sich so (fast) immer vorhersagen.[42] Dieses Wissen können die Inhaber der Daten für ihre Zwecke benutzen, um den Betroffenen in seinem Verhalten durch Informationssteuerung zu beeinflussen. Er wird gar nicht merken, dass ihm genau die Information angeboten wird, die sein gewünschtes Verhalten bewirkt, sondern dieses für eine vollkommen freie Entscheidung halten.

In vielen Fällen kann die Unsicherheit darüber, was der Gegenüber – der Arbeitsgeber, der staatliche Beamte, der Bankmitarbeiter, der über einen Kredit entscheidet – weiß, dazu führen, dass

40 Fabian/Günter/Spiekermann 2005.

41 S. z.B. Mattern 2003c, 31; Mattern 2004, 328.

42 SWAMI 2006c, 8.

man sich so verhält, wie man es vermutet, dass es der andere erwartet. Wenn man weiß, dass man durch technische Systeme beobachtet werden kann, werden sich viele – wie das Bundesverfassungsgericht befürchtet[43] – so verhalten, dass sie nicht auffallen.[44] Auf diese Weise kann allein durch die Überwachungsarchitektur das Verhalten von vielen Menschen gesteuert werden.

Die Systeme allgegenwärtiger Datenverarbeitung könnten aber auch und gerade bei Kenntnis ihrer Datenerhebung und -nutzung durch den objektiven Zwang ihrer Strukturen das Verhalten des Betroffenen beeinflussen. Sind Systeme der allgegenwärtigen Datenverarbeitung in bestimmten Lebensbereichen tatsächlich ubiquitär, hat der Betroffene nämlich gar keine Chance, sich der Datenverarbeitung zu widersetzen oder ihr aus dem Weg zu gehen. Realistisch betrachtet wird der Betroffene in vielen Fällen sein allgemeines Persönlichkeitsrecht zurückstellen, um nicht finanzielle oder gesellschaftliche Nachteile in Kauf nehmen zu müssen. Die Einführung von Ubiquitous Computing in bestimmten Kontexten kann den Bürger damit in die Zwangslage bringen, zwischen zwei möglicherweise gravierenden Übeln wählen zu müssen. Dies wäre eine gravierende Einschränkung heute bestehender Entscheidungsalternativen.[45]

In allen gesellschaftlichen Bereichen wird die Möglichkeit der Entscheidungs- und Entfaltungsfreiheit dadurch unterstützt, dass mit der Zeit viele Informationen über andere Personen vergessen werden. Im Zeitalter der automatischen Datenverarbeitung wird dieses Vergessen durch Löschungsregelungen nachgebildet.[46] Diese Entlastung des gesellschaftlichen Zusammenlebens könnte jedoch unmöglich werden, wenn in Anwendungen allgegenwärtiger Datenverarbeitung das regelmäßige Löschen von perso-

43 BVerfGE 65, 1 (43).

44 S. auch UNESCO 2007, 48, für beobachtete Mitarbeiter.

45 S. auch UNESCO 2007, 48f.; zu dem damit verbunden »Gefühl der Unfreiheit« s. Möller/Bizer, in: TAUCIS 2006, 115.

46 Z.B. Löschung von Verkehrsverstößen im Flensburger Bundeszentralregister, Löschung von Einträgen im Bundeszentralregister.

nenbezogenen Daten nicht entsprechend realisiert wäre. Unter diesen Bedingungen dürfte das Gefühl der Menschen wachsen, der Technik ausgeliefert zu sein und permanent kontrolliert zu werden. Dieses Gefühl kann zu Verhaltensänderungen des Beobachteten führen, mit der Folge, dass dieser sich in der Beobachtungssituation nicht entsprechend seines freien Willens, sondern nach vermuteten Erwartungshaltungen verhalten wird.[47]

2.5 Allgegenwärtige Überwachung

Mit Ubiquitous Computing wird eine potenziell perfekte Überwachungsinfrastruktur aufgebaut.[48] Die Anwendungen allgegenwärtiger Datenverarbeitung werden eingeführt, um die Sinne und das Gedächtnis ihrer Nutzer zu erweitern. Diese Erweiterung werden sie zur Kontrolle ihrer Umwelt nutzen. Sie wollen dieser Technik ihre Sicherheit anvertrauen und in ihrem Kontrollbedürfnis durch sie entlastet werden. Wenn allgegenwärtige Datenverarbeitung so funktioniert, wie sie soll, funktioniert sie immer auch als Überwachungstechnologie.

Wenn kleinste Sensorchips ein billiges Massenprodukt werden, dann lässt sich ihr Einsatz kaum mehr kontrollieren und ein Missbrauch zu Kontrollzwecken nur schwer verhindern.[49] Sie werden als effektive Überwachungstechnologie nicht nur den unter engen Bedingungen dazu legitimierten und verantwortlichen staatlichen Organen zur Verfügung stehen, sondern jedem, der ein Überwachungsinteresse hat.

Werden sie als Sensornetze ausgebracht, werden sie nicht nur Naturphänomene oder den Zustand von Gegenständen beobachten, sondern auch direkt oder indirekt das Verhalten von Menschen

47 S. hierzu auch Möller/Bizer, in: TAUCIS 2006, 115.

48 S. hierzu auch Roßnagel, it 2007, 83 ff.; Roßnagel 2003e, 25 ff.; Roßnagel, EuZ 2006, 35; Langheinrich 2005a, 336f.; Mattern 2003c, 31f.; Mattern 2004, 328.

49 S. Mattern 2005b, 60.

oder Gruppen.[50] Sie ermöglichen eine unbemerkte, räumlich und zeitlich vollständige Überwachung eines bestimmten Gebiets. Sie bilden dann einen wichtigen Teil der räumlichen Überwachungsinfrastruktur. Wenn sie viele Daten über das Geschehen in ihrer Umgebung speichern, kann theoretisch jeder beliebige Zustand rekonstruiert werden, weil die Sensordaten zu einem bestimmten Ort zu einer bestimmten Zeit oder einem bestimmten Zeitraum wiedergegeben werden können. Mit ihrer Hilfe kann rekonstruiert werden, wann sich Menschen wo wie lange aufgehalten haben, ob sie sich unterhalten haben oder sonstigen Tätigkeiten nachgegangen sind. Diese Sensordaten können ihnen individuell zugeordnet werden, wenn charakteristische biometrische Merkmale wie etwa Größe und Gewicht oder Spezifika des Gangs oder anderer Bewegungsbilder aufgenommen oder andere Identifizierungsmittel verwendet werden. Durch Sensornetzwerke werden die qualitativen und quantitativen Möglichkeiten der Überwachung derart ausgeweitet, dass auch Bereiche erfasst werden, die einem dauerhaften und unauffälligen Monitoring bisher nicht zugänglich waren.[51] Schließlich sind Sensorchips nahezu unsichtbare, aber äußerst effektive »Spione«.

Ebenso wie Sensornetze können auch die Infrastrukturen anderer Anwendungen allgegenwärtiger Datenverarbeitung für Überwachungszwecke genutzt werden. Dies gilt beispielsweise für Lokalisierungssysteme,[52] RFID-Systeme, Gebäudesysteme, Verkehrstelematiksysteme oder für persönliche virtuelle »Tagebücher«. Sie alle sind für Überwachungsaufgaben konstruiert und können daher grundsätzlich für beliebige Überwachungsfunktionen zum Einsatz kommen.

Bestehen Interessen zur Aufklärung einer Straftat oder zur Sicherheitsvorsorge, entsteht immer ein Druck, die Daten aus sol-

50 S. z.B. Mattern 2003c, 19; Mattern 2005b, 60.

51 Mattern 2005b, 60 hält sie daher langfristig für eine größere Bedrohung als die in dieser Hinsicht derzeit kontrovers diskutierte RFID-Technologie.

52 S. Dobson/Fisher 2003: »Society must contemplate a new form of slavery, characterized by location control«; s. auch Mattern 2007a, 22.

chen Überwachungssystemen auch auszuwerten und zu nutzen. Infrastrukturen der allgegenwärtigen Datenverarbeitung vergrößern somit enorm die technische Überwachungskapazität – ohne dass hierfür Menschen eingesetzt werden müssen und dass die Beobachteten etwas merken. Durch sie kann eine permanente, umfassende, unmerkliche Beobachtung realisiert werden.[53]

Durch die Pflicht von Anbietern öffentlicher Kommunikationsdienste zur Vorratsspeicherung aller Kommunikationsdaten wurde für staatliche Überwachungsbehörden in Europa bereits ein Zugang zu dieser neuen Überwachungsinfrastruktur eröffnet.[54] Er war vielleicht nicht für allgegenwärtige Datenverarbeitung gedacht, aber diese wird mit ihrer Entfaltung und Verbreitung in den Anwendungsbereich der Vorratsspeicherungspflicht und der staatlichen Überwachungsbefugnisse hineinwachsen. Auch ist nicht auszuschließen, dass neue Gesetze dazu zwingen, die Logfiles aller Transaktionen allgegenwärtiger Datenverarbeitung über einen längeren Zeitraum aufzubewahren und den Strafverfolgungsbehörden auf Verlangen zur Verfügung zu stellen.[55]

[53] S. z.B. Cas 2002.

[54] S. Richtlinie 2006/24/EG vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, EU ABl. L 105/54; s. hierzu Roßnagel, EuZ 2006, 30 ff.

[55] So BSI 2004, 102f. für RFID-Daten im Rahmen eines Szenarios.

3. SCHUTZ DER INFORMATIONELLEN SELBSTBESTIMMUNG?

Allgegenwärtige Datenverarbeitung hat ambivalente Potentiale. Sie verspricht, Träume verwirklichen zu können, mit ihr als Mittel ließen sich aber auch Alpträume realisieren. Niemand weiß, welche Potentiale unter welchen Umständen zukünftig realisiert werden. Wenn wir Einfluss auf unsere Zukunft nehmen wollen, müssen wir beide Möglichkeiten ernst nehmen. Die mögliche Entwicklung zu ignorieren, die zu Grundrechtseinschränkungen und Demokratieverlusten führen könnte, wäre genauso falsch, wie sich nur auf die Nachteile zu fixieren. Daher ist die Frage zu stellen, inwieweit das Recht in der Lage ist, freiheitseinschränkende Entwicklungen zu verhindern und freiheitsförderliche zu unterstützen.

In diesem Kapitel wird untersucht, ob das Datenschutzrecht und sein staatlicher oder privater Vollzug zumindest für den Schutz der informationellen Selbstbestimmung diese Ambivalenz der Potenziale aufheben kann. Im Folgenden wird das Schutzgut der informationellen Selbstbestimmung und das datenschutzgesetzliche Programm zu seinem Schutz dargestellt und seine Leistungsfähigkeit in einem informatisierten Alltag untersucht.

Aus Sicht der Selbstbestimmung und ihres Schutzes kann der bereits beschriebene Entwicklungssprung der Informationstechnik kaum überbewertet werden. Denn er fordert vom Datenschutzrecht ebenfalls einen Entwicklungssprung, um mit den technikbedingten Bedrohungen mithalten zu können. Dies wird deutlich, wenn die bisherigen Stufen der gemeinsamen Entwicklung von Informationstechnik und Datenschutz in Erinnerung gerufen werden.

In einer ersten Stufe der Entwicklung von Informationstechnik und Datenschutzrecht 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. Wurde die Zweckbindung beachtet, wusste der Betroffene in der Regel, wo welche Daten über ihn verarbeitet wurden. Für diese Stufe der Datenverarbeitung sind die Schutzkonzepte der ursprünglichen Datenschutzgesetze entwickelt worden.[1] Aus dieser Zeit stammen die Regelungen zur Zulässigkeit der Datenverwendung, die Anforderung an Unterrichtung und Benachrichtigung, an Zweckbestimmung und Zweckbindung, an die Erforderlichkeit der Datenverwendung, an die Rechte der Betroffenen und die Kontrolle durch Aufsichtsbehörden. Die Nutzung von PCs hat die Datenschutzrisiken zwar erhöht, aber nicht auf eine neue qualitative Stufe gehoben.

Die zweite, qualitativ neue Stufe der Datenverarbeitung 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.[2] Jede Handlung in diesem viele Lebensbereiche erfassenden Cyberspace hinterlässt Datenspuren, die ausgewertet werden können und auch werden.[3] Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können vom Betroffenen kontrolliert werden. Für die Datenverarbeitung in Deutschland versuchen die Multimedia-Datenschutzgesetze, die Risiken in den Griff zu bekommen.[4]

[1] 1971 trat das Hessische Datenschutzgesetz als erstes Datenschutzgesetz der Welt und 1978 das Bundesdatenschutzgesetz (BDSG) in Kraft. Auch die 1995 in Kraft getretene europäische Datenschutz-Richtlinie gehört zur Generation dieser Datenschutzgesetze und setzt im Wesentlichen die deutschen Datenschutzansätze in der Europäischen Gemeinschaft um.

[2] S. hierzu näher Roßnagel, ZRP 1997, 26.

[3] S. näher Roßnagel/Banzhaf/Grimm 2003, 55 ff.

[4] S. Roßnagel, in: Roßnagel 2003a, 1280 ff.

Sie haben für die Internetdienste die Anforderungen an Transparenz, Zweckbindung und Erforderlichkeit verschärft und vor allem das neue Prinzip der Datensparsamkeit eingeführt. Diese normativen Vorgaben können allerdings nur im Wirkungsbereich des Nationalstaats zur Geltung gebracht werden. Die neue Datenverarbeitung betrifft je nach Nutzung des Internet einen großen oder kleinen Ausschnitt des täglichen Lebens, diesen aber potenziell vollständig. Allerdings kann der Betroffene den Risiken des Internets zumindest noch dadurch entgehen, dass er diesen virtuellen Sozialraum meidet.

Mit 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 Welt verfügbar, Informationen aus der realen Welt werden in die virtuelle Welt integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es aber keinen Ausweg mehr.[5] Insofern verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell. Für diese neuen Herausforderungen gibt es keine spezifischen Regelungen. Solche werden zwar gefordert,[6] von der Bundesregierung aber (noch) nicht als notwendig angesehen.[7]

3.1 Das Schutzgut der informationellen Selbstbestimmung

Für den Schutz der Selbstbestimmung ist Datenschutz eigentlich ein irreführender Begriff. Durch Datenschutz und Datenschutzrecht sollen nämlich nicht die Daten (des Datenbesitzers) ge-

[5] Ebenso Langheinrich 2005a, 336.

[6] S. zum Beispiel das Gutachten von Roßnagel/Pfitzmann/Garstka 2001, das 15, 22f., 28, 42, 60, 63, 113 und 115 Anforderungen des Ubiquitous Computing berücksichtigt.

[7] S. die Antwort der Bundesregierung 2004, BT-Drs. 15/3190, auf eine kleine Anfrage der FDP-Fraktion.

schützt werden, sondern die informationelle Selbstbestimmung (des Betroffenen – vorrangig gegen den Datenverarbeiter).[8] Datenschutz ist daher keine Frage des Schutzes von Verfügungsrechten, sondern der Freiheit.

»Individuelle Selbstbestimmung« so das Bundesverfassungsgericht in seiner bahnbrechenden Entscheidung zur Volkszählung 1983 – »setzt … – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten«. Wer (aber) »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.«[9]

Als die verfassungsrechtliche Antwort auf »die modernen Bedingungen der Datenverarbeitung« hat das Bundesverfassungsgericht daher die informationelle Selbstbestimmung als Grundrecht anerkannt.[10] »Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.«[11] Die informationelle Selbstbestimmung ist – neben der Informationsfreiheit und dem Telekommunikationsgeheimnis – das zentrale Grundrecht der Informationsgesellschaft.[12] Sie hat eine subjektive und eine objektive Schutzrichtung.

[8] S. näher Roßnagel, Informatik Spektrum 2005, 462 ff.

[9] BVerfGE 65, 1 (43).

[10] Ständige Rechtsprechung des BVerfG – s. z.B. jüngst BVerfG, NJW 2006, 976 (978), Rn. 85; BVerfG, NJW 2006, 1939 (1940), Rn. 66 und 68.

[11] BVerfGE 65, 1 (43); 78, 77 (84); 84, 192 (194); 96, 171 (181); 103, 21 (32f.); 113, 29 (46); BVerfG, NJW 2006, 976 (978), Rn. 85; BVerfG, NJW 2006, 1939 (1940), Rn. 69.

[12] S. näher Trute 2003, 156 ff.; Hornung, MMR 2004, 3 ff.

3.1.1 Subjektives Grundrecht

Die informationelle Selbstbestimmung schützt einmal die selbstbestimmte Entwicklung und Entfaltung des Einzelnen. Seine Persönlichkeit wird geprägt durch das Gesamtbild des Handelns und Kommunizierens in unterschiedlichen sozialen Rollen. Sie setzt für ihre Entfaltung voraus, dass er sich in diesen Rollen darstellen kann und ihm diese Selbstdarstellung in der Kommunikation mit anderen zurückgespiegelt wird. Individuelle Entwicklung und Entfaltung kann nur gelingen, wenn der Betroffene die Preisgabe von Angaben über sich kontrollieren kann. Kann er diese aber nicht erkennen, kann er »in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden«.[13] Dementsprechend muss der Einzelne in der Lage sein, selbst zu entscheiden, welche Daten er über sich in welcher Rolle und in welcher Kommunikation preisgibt. Diesen Vorrang autonomer Entscheidung über Informationsfreigaben schützt das Grundrecht auf informationelle Selbstbestimmung.

In dieses Grundrecht greift derjenige ein, der Daten der betroffenen Person gegen ihren Willen verarbeitet – unabhängig davon, ob dies eine staatliche Behörde oder ein privates Unternehmen ist.[14] Die betroffene Person ist in beiden Fällen gleich schutzwürdig. Die Missachtung ihrer informationellen Selbstbestimmung ist in beiden Fällen ein Eingriff.[15] Allerdings begründet das Grundrecht nur gegenüber der staatlichen Gewalt eine unmittelbare Abwehrfunktion. Für private Unternehmen ist zu berücksichtigen, dass sie sich ebenfalls auf Grundrechte – hier vor allem die Freiheit der Berufsausübung – berufen können. Allerdings ermächtigen die Grundrechte nicht dazu, in andere Grundrechte einzugreifen. Vielmehr ist es Aufgabe des Gesetzgebers, konkurrierende Grundrechtssphären so abzugrenzen, dass die

[13] BVerfGE 65, 1 (43).

[14] Ebenso z.B. Simitis, NJW 1984, 401; Hoffmann-Riem 1997, 784; Hoffmann-Riem, AöR 1998, 524; Schulz, Verwaltung 1999, 143; Kunig, Jura 1993, 602; a.A. z.B. Ehmann, RDV 1988, 169 ff., 221 ff.

[15] BVerfGE 84, 192 (195).

Ausübung von Grundrechten nicht dazu führt, dass dadurch in die Grundrechte anderer eingegriffen wird. Soweit der Gesetzgeber nicht das Grundrecht auf informationelle Selbstbestimmung zugunsten überwiegender privater Interessen durch Gesetze eingeschränkt hat, haben Private kein eigenständiges Recht zur Verarbeitung personenbezogener Daten Dritter.[16]

3.1.2 Objektives Strukturprinzip einer Kommunikationsverfassung

Informationelle Selbstbestimmung ist nicht nur ein subjektives Recht des jeweils Betroffenen, sondern zugleich auch die Grundlage einer freien und demokratischen Kommunikationsverfassung. »Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. … Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist.«[17] »Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß.«[18] Informationelle Selbstbestimmung zielt somit auf eine Kommunikationsordnung, die einen selbstbestimmten Informationsaustausch und eine freie demokratische Willensbildung ermöglicht.

In dieser überindividuellen Funktion ist die informationelle Selbstbestimmung auch Element einer »objektiven Wertordnung«, »die als verfassungsrechtliche Grundentscheidung für

[16] S. z.B. Roßnagel/Pfitzmann/Garstka 2001, 46 ff.
[17] BVerfGE 65, 1 (43); BVerfG, NJW 2006, 976 (979), Rn. 87
[18] BVerfG, NJW 2006, 976 (979), Rn. 86.

alle Bereiche des Rechts gilt und Richtlinien und Impulse für Gesetzgebung, Verwaltung und Rechtsprechung gibt«.[19] Sie und die anderen Grundrechte bilden zentrale Grundpfeiler einer freien gesellschaftlichen Ordnung. Sie sind bei der Interpretation aller Rechtsnormen zu beachten und füllen vor allem die inhaltlich offenen Normen des Privatrechts aus.

3.1.3 Kommunikationsordnung auf der Basis der Selbstbestimmung

Die informationelle Selbstbestimmung unterliegt vielfach zwei Missverständnissen. Zum einen wird sie oft als »Property Right«[20] missverstanden. Informationelle Selbstbestimmung schützt jedoch nicht Verfügungsrechte, sondern Freiheit.[21] Sie begründet kein eigentumsähnliches Herrschaftsrecht über personenbezogene Daten.[22] Sie ist als Funktionsvoraussetzung einer freien und demokratischen Gesellschaft nicht in das – vom richtigen Preis abhängige – Belieben des Individuums als Händler seiner Daten gestellt. Ein solches Missverständnis würde auch dem Charakter personenbezogener Daten als mehrrelationales Modell der Wirklichkeit nicht gerecht.[23] So »gehören« – etwa im Beispiel des Ubiquitous Computing im Straßenverkehr – Wartungsdaten eines Kraftfahrzeugs nicht nur dessen Eigentümer, sondern auch dem Reparaturbetrieb. Eine ausschließliche Zuordnung zu einem – dem Autor oder dem Objekt des Wirklichkeitsmodells »Wartung des Autos« – ist nicht möglich.[24] Ebenso sind zum Beispiel Gesundheitsdaten nicht Eigentum des Patienten, auch nicht des Arztes. Vielmehr ist eine Informations- und Kommunikationsordnung gefragt, die bestimmt, wer in welcher Beziehung

[19] BVerfGE 39, 1 (41) – Hervorhebung durch den Verfasser.
[20] Samuelson 2000; Kilian 2002.
[21] BVerfGE 65, 1 (44).
[22] Obwohl ein gesellschaftlicher Trend dahin zu gehen scheint, Datenschutz zur Selbstdarstellung (Web 2.0) oder für geringe finanzielle Vorteile (Kundenkarten) bewusst aufzugeben – s. hierzu Mattern 2007a, 21.
[23] S. z.B. Steinmüller 1993, 216 ff.
[24] BVerfGE 65, 1 (44).

befugt ist, mit dem Modell in einer bestimmten Weise umzugehen. Diese Ordnung soll auf dem Prinzip der informationellen Selbstbestimmung aufgebaut sein – mit den genannten Kommunikationsmöglichkeiten im überwiegenden Individual- oder Allgemeininteresse.

Das zweite Missverständnis geht in die gegenteilige Richtung, nämlich die Gleichsetzung von informationeller Selbstbestimmung und »Privacy«. Im Gegensatz zum europäischen Konzept der informationellen Selbstbestimmung als Grundlage einer Kommunikationsordnung entspricht das amerikanische Konzept der Privacy in seinem Kerngehalt dem »right to be let alone«.[25] Dieses zielt auf Ausschluss von Kommunikation, auf das Recht zum Rückzug aus der Gesellschaft. Dagegen soll die auf Selbstbestimmung aufbauende Kommunikationsordnung Kommunikation nicht unterbinden, sondern – allerdings selbstbestimmt – ermöglichen. Datenschutz bezweckt nicht den Schutz des Eigenbrötlers, der sich von der Welt abschotten will, sondern den Schutz des selbstbestimmt in der Gesellschaft Agierenden und Kommunizierenden.

3.1.4 Ergänzender Grundrechtsschutz

Allgegenwärtige Datenverarbeitung wird nicht nur die informationelle Selbstbestimmung berühren, sondern auch weitere Grundrechte wie das Fernmeldegeheimnis des Art. 10 Abs. 1 GG oder das Wohnungsgrundrecht des Art. 13 GG. Hinsichtlich der Datenerhebung und -verarbeitung in der allgegenwärtigen Datenverarbeitung wirken diese Grundrechte eng mit dem Grundrecht auf informationelle Selbstbestimmung zum Freiheitsschutz des Betroffenen zusammen und sollen daher kurz vorgestellt werden.

[25] Warren/Brandeis, Harvard Law Review 4 (1890), 193 ff.; Solove, Univesity of Pennsylvania Law Review 154 (2006), 477 ff.

»Art. 10 GG schützt die private Fernkommunikation.« Das Grundrecht gewährleistet »die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter – einschließlich staatlicher Stellen – ermöglicht«. Es schützt »vor ungewollter Informationserhebung und gewährleistet eine Privatheit auf Distanz«.[26] »Das Grundrecht ist entwicklungsoffen und umfasst … auch neuartige Übertragungstechniken.«[27]

»Das Fernmeldegeheimnis umfasst nicht nur den Kommunikationsinhalt, sondern schützt auch die Kommunikationsumstände.«[28] Dazu gehören auch die Verkehrsdaten, die bei digitalisierten Kommunikationsvorgängen entstehen.[29] Insofern »enthält Art. 10 GG bezogen auf den Fernmeldeverkehr eine spezielle Garantie, die die allgemeine Gewährleistung des Rechts auf informationelle Selbstbestimmung verdrängt«.[30] Allerdings gelten insoweit die Grundsätze, die für das Recht auf informationelle Selbstbestimmung aufgestellt worden sind, auch für den Schutz des Fernmeldegeheimnisses in Art. 10 GG.[31]

Allerdings sind für die Geltung des Fernmeldegeheimnisses zwei wichtige Einschränkungen zu beachten, die für allgegenwärtige Datenverarbeitung besondere Relevanz haben.

Erstens gilt Art. 10 GG nicht für die Daten, die in den Endgeräten der Teilnehmer über die Kommunikation gespeichert sind. Sie unterfallen nur dem Recht auf informationelle Selbstbestim-

[26] BVerfG, NJW 2006, 976 (978), Rn. 65.

[27] BVerfGE 46, 120 (144); 106, 28 (36); BVerfG, NJW 2006, 976 (978), Rn. 67.

[28] BVerfGE 100, 313 (358); BVerfGE, NJW 2006, 976 (978), Rn. 68; BVerfG, NJW 2006, 3197.

[29] BVerfGE 67, 157 (172); 85, 386 (396); 110, 33 (53); BVerfGE, NJW 2005, 2603 (2604); BVerfGE, NJW 2006, 976 (978), Rn. 70.

[30] BVerfGE 67, 157 (171); 100, 313 (358); 107, 299 (312); 110, 33 (53); BVerfG, NJW 2005, 2603 (2604); BVerfG, NJW 2006, 976 (979), Rn. 88.

[31] BVerfGE 100, 313 (359); 110, 33 (53); BVerfG, NJW 2006, 976 (979f.), Rn. 88.

mung.[32] Daten aus einer Kommunikation zwischen einem Nutzer und seinem kommunikationsfähigen Gerät, die das Gerät speichert, sind nicht durch Art. 10 GG, sondern durch die informationelle Selbstbestimmung geschützt.

Zweitens gilt Art. 10 GG nicht für den Kommunikationsvorgang zwischen zwei Geräten. »Art. 10 Abs. 1 GG folgt nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes,[33] sondern knüpft personal an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an.«[34] Der Schutz des Fernmeldegeheimnisses umfasst daher nur die menschliche Kommunikation. Schon gar nicht greift Art. 10 Abs. 1 GG, wenn die Kommunikation zwischen Geräten – ohne Einschaltung eines Telekommunikationsunternehmens – direkt stattfindet.[35]

Sofern allgegenwärtige Datenverarbeitung in der Wohnung stattfindet, ist das Grundrecht auf Unverletzlichkeit der Wohnung zu beachten. Es verbürgt dem Einzelnen einen elementaren Lebensraum und gewährleistet das Recht, in ihm in Ruhe gelassen zu werden.[36] Geschützt wird die »räumliche Privatsphäre«.[37] Unter den Bedingungen moderner Überwachungstechnologien würde jedoch »der Schutzzweck der Grundrechtsnorm vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Art. 13 Abs. 1 GG umfasst wäre«.[38] Daher sind Auswertungen von Anwendungen allgegenwärtiger Datenverarbeitung, die in einer Wohnung stattfinden, am Grundrecht aus Art. 13 Abs. 1 GG zu messen.

[32] BVerfGE, NJW 2006, 976 (978), Rn. 72 ff.
[33] S. § 3 Nr. 22 TKG.
[34] BVerfG, K&R 2007, 32 (35)
[35] BVerfG, K&R 2007, 32 (36).
[36] BVerfGE 32, 54 (75); 42, 212 (219); 51, 97 (110); 109, 279 (309).
[37] BVerfGE 7, 230 (238); 109, 279 (319, 327).
[38] BVerfGE 109, 279 (309); s. hierzu auch Jahn/Kudlich, JR 2007, 60; Bär, MMR 2007, 176; Hornung 2007, i.E.

Im Folgenden wird vor allem das Verhältnis zwischen allgegenwärtiger Datenverarbeitung und informationeller Selbstbestimmung und ihrer Ausprägung im Schutzprogramm des Datenschutzrechts untersucht, weil das Fernmeldegeheimnis und das Wohnungsgrundrecht nur bei speziellen Fallkonstellationen zum Tragen kommen und der Eingriff in diese speziellen Grundrechte an vergleichbaren Maßstäben zu messen wäre.

3.2 Schutzkonzept des Datenschutzrechts

Das Grundrecht auf informationelle Selbstbestimmung entfaltet eine Abwehrfunktion gegenüber staatlichen Eingriffen und eine Schutzfunktion des Staates gegenüber privaten Eingriffen. Um das Grundrecht wirksam werden zu lassen, hat das Bundesverfassungsgericht in mehreren Entscheidungen Anforderungen zu seinem Schutz abgeleitet. Die Vorschriften des Datenschutzrechts können vielfach als Umsetzung dieses normativen Schutzprogramms verstanden werden. Sie entsprechen auch den Grundprinzipien des Datenschutzes nach der Europäischen Datenschutzrichtlinie. Die wesentlichen Bestandteile dieses Schutzprogramms sind die folgenden:

3.2.1 Besondere Zulassung

Jede Verwendung personenbezogener Daten ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung.[39] Sie ist daher nur zulässig, wenn der Gesetzgeber oder der Betroffene sie hinsichtlich Umfang und Zweck gebilligt haben.[40] Der Betroffene muss hierüber vor der Einwilligung unterrichtet worden sein. Er muss die Einwilligung freiwillig und in einer bestimmten Form abgeben. Diese Form ist im Regelfall die Schriftform mit eigen-

[39] S. BVerfGE 100, 313 (366); dies gilt auch für die Datenverwendung durch private Stellen – s. BVerfGE 84, 192 (195).
[40] S. näher Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 36f.

händiger Unterschrift oder die elektronische Form mit qualifizierter elektronischer Signatur.[41]

3.2.2 Transparenz

Die betroffene Person kann nur überprüfen, ob die Datenverarbeitung rechtmäßig ist, und ihre Rechte wahrnehmen, wenn die Datenverarbeitung ihr gegenüber transparent ist.[42] Ohne Transparenz wird die betroffene Person faktisch rechtlos gestellt. Daher sind die Daten grundsätzlich bei der betroffenen Person zu erheben. Diese ist vor der Erhebung zu unterrichten, bei einer neuen Speicherung zu benachrichtigen und hat gegenüber der verantwortlichen Stelle Auskunftsrechte.[43]

3.2.3 Zweckbindung

Das Gesetz oder die Einwilligung erlauben die Datenverwendung nur zu einem bestimmten Zweck.[44] Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten ist auf diesen Zweck begrenzt. Eine Zweckänderung bedarf einer eigenen Erlaubnis. Die betroffene Person soll in der Lage sein, die sie betreffenden Daten entsprechend ihrer sozialen Rolle im jeweiligen sozialen Kontext selbst zu steuern.[45] Infolge dieser Zweckbindung sind eine informationelle Gewaltenteilung sicherzustellen, die Daten gegenüber Unberechtigten abzuschotten und ein Zugriffsschutz zu gewährleisten.[46] Eine Datenverarbeitung auf

41 S. z.B. Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 38 ff.; Holznagel/Sonntag, in: Roßnagel 2003a, 685 ff.; für die europäische Ebene Artikel-29-Datenschutzgruppe 2005a, 10f.

42 S. BVerfGE 65, 1 (46, 59).

43 S. hierzu z.B. Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 41f.; Wedde, in: Roßnagel 2003a, 547 ff.; für die europäische Ebene Artikel-29-Datenschutzgruppe 2005a, 11f.

44 S. BVerfGE 65, 1 (46).

45 S. hierzu näher Zezschwitz, in: Roßnagel 2003a, 221 ff.

46 S. BVerfGE 65, 1 (49).

Vorrat ist untersagt und die Bildung umfassender Profile verboten.[47]

3.2.4 Erforderlichkeit

Jede Verarbeitung personenbezogener Daten ist nur zulässig, soweit sie erforderlich ist, um den zulässigen Zweck zu erreichen: Es dürfen nur die Daten verarbeitet werden, die für das Erreichen des Zwecks unabdingbar sind.[48] Die Datenverarbeitung ist auf die Phasen zu beschränken, die für das Erreichen des Zwecks notwendig sind. Sind die Daten nicht mehr erforderlich, sind sie zu löschen.[49]

3.2.5 Mitwirkung

Informationelle Selbstbestimmung ist nur möglich, wenn die betroffene Person Mitwirkungsmöglichkeiten hat und die Datenverarbeitung beeinflussen kann. Daher hat die betroffene Person Auskunftsrechte, Korrekturrechte hinsichtlich Berichtigung, Sperrung und Löschung sowie das Recht zum Widerspruch. Sie kann Schadensersatz einfordern, wenn sie durch eine unzulässige oder unrichtige Verarbeitung personenbezogener Daten einen Schaden erleidet.[50]

3.2.6 Kontrolle

Ohne Stellen, die die Einhaltung der Rechte und Pflichten des Datenschutzrechts überwachen, wäre deren Durchsetzung gefährdet. Bei der »für den Bürger bestehenden Undurchsichtigkeit der

47 S. S. BVerfGE 65, 1 (46, 52f.); Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 41f.; Scholz, in: Roßnagel 2003a, 1845 ff.

48 S. BVerfGE 65, 1 (46).

49 BVerfGE 65, 1 (46); Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 43 ff.

50 S. näher z.B. Wedde 2003, 554 ff.; Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 47.

Speicherung und Verwendung von Daten« ist für einen effektiven Schutz der informationellen Selbstbestimmung die flankierende Beteiligung unabhängiger Datenschutzkontrolleinrichtungen erforderlich.[51] Sie müssen dem Betroffenen bei der Durchsetzung seiner Rechte behilflich sein und auch von sich aus in vorbeugender Weise die Einhaltung der Datenschutzbestimmungen überwachen.[52] Datenschutzkontrolle kann in Form der Fremdkontrolle durch unabhängige Kontrollstellen, aber auch in Form der Selbstkontrolle durch betriebliche und behördliche Datenschutzbeauftragte stattfinden. Die internen Beauftragten beraten die verantwortliche Stelle bei der Entwicklung und Auswahl von Datenverarbeitungssystemen, beim Wirkbetrieb der Systeme, bei organisatorischen Änderungen, bei der Erstellung unternehmensinterner Richtlinien und Anweisungen, bei der Information über Datenschutzfragen sowie in Einzelfällen. Außerdem führen sie bei besonderen Risiken für die Rechte und Freiheiten der Betroffenen Vorabkontrollen der Datenverarbeitungssysteme durch.[53]

3.2.7 Selbst- und Systemdatenschutz

Diesem Schutzprogramm der ersten Entwicklungsstufe hat die Diskussion um die informationelle Selbstbestimmung im Internet, also in der zweiten Entwicklungsstufe, vor allem einen ersten Schritt hin zu einer Einbettung von Datenschutz in Technik hinzugefügt.[54] Die erste Ausprägung des Datenschutzes durch Technik ist der Selbstdatenschutz.[55] Dem Betroffenen sollen eigene Instrumente in die Hand gegeben werden, seine informationelle Selbstbestimmung selbst zu schützen. Selbstdatenschutz kann vor allem durch technische Möglichkeiten des anonymen

[51] BVerfGE 65, 1 (46, 59).

[52] S. hierzu Heil, Garstka/Gill und Hillenbrandt-Beck, in: Roßnagel 2003a, 748 ff.

[53] S. hierzu näher Königshofen und Abel, in: Roßnagel 2003a, 857 ff.

[54] S. z.B. Bäumler, DuD 1999, 258; Schaar 2003, § 4 TDDSG, Rn. 307 ff.

[55] S. näher Roßnagel 2003c, 325 ff.

und pseudonymen Handelns verbessert werden. Eine andere Ausprägung des Datenschutzes durch Technik ist der Systemdatenschutz.[56] Er soll durch Gestaltung der Datenverarbeitungssysteme vor allem erreichen, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden.[57] Darüber hinaus kann Systemdatenschutz zur Umsetzung weiterer datenschutzrechtlicher Ziele wie der informationellen Gewaltenteilung oder der Transparenz und Kontrolleignung der Datenverarbeitung eingesetzt werden.

3.2.8 Das System des Datenschutzes

Zusammenfassend ist festzuhalten, dass Datenschutz nicht auf den Schutz der Daten im Sinn der ausschließlichen Verfügung über die Daten durch den Datenverarbeiter zielt – dies betrifft allenfalls Fragen der Datensicherheit, sondern letztlich auf eine freie Kommunikationsverfassung der Gesellschaft. Es geht um die Frage, wer über welche personenbezogenen Daten verfügen und diese in gesellschaftlicher Kommunikation verwenden können soll. Diese Frage muss vom Prinzip der informationellen Selbstbestimmung der betroffenen Person her beantwortet werden, wenn Freiheit und Demokratie in der Gesellschaft wirklich sein sollen. Die Antwort ist dahingehend zu operationalisieren, dass die beschriebenen Funktionen der Transparenz, Zweckbindung, Erforderlichkeit, Mitwirkung und Kontrolle bei allen Formen der Verarbeitung personenbezogener Daten gewährleistet werden müssen.

3.3 Eignung normativen Schutzes

Das Datenschutzrecht enthält zwar keine speziellen Regelungen für Anwendungen allgegenwärtigen Rechnens. Sein normatives

[56] S. näher Dix, in: Roßnagel 2003a, 363 ff.

[57] Zur Datenvermeidung und Datensparsamkeit s. auch Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 45; Bizer 2006, § 3a Rn. 34 ff.

Schutzkonzept kann aber grundsätzlich auch für die Anwendungen taugliche normative Lösungen bieten, die erwartbare Interessenkonflikte in akzeptabler Weise regeln.[58]

3.3.1 Allgegenwärtige Datenverarbeitung in überschaubaren Strukturen

Die Eignung des normativen Schutzes durch Datenschutzrecht setzt aber voraus, dass

- nur wenige Instanzen mit klarer Rollenzuweisung beteiligt sind. Soweit der Staat Überwachungsdaten erhebt, der Arbeitgeber mit Logistikdaten auch Daten seines Arbeitnehmers speichert, der Vermieter in seinem Haus Daten über den individuellen Energieverbrauch seiner Mieter verarbeitet, der Verkäufer dem Kunden nur mit RFID-Chips versehene Waren anbietet, oder die Autoversicherung das Fahrverhalten der Versicherungsnehmer für die Prämienberechnung aufzeichnet, besteht eine klare und einfache »Frontstellung« zwischen Datenverarbeiter und Betroffenem.
- die Verhältnisse überschaubar sind. Soweit nur wenige Beteiligte einzelne Schritte der Datenerhebung, -verarbeitung und -nutzung durchführen und damit eindeutige Zwecke verfolgen, herrschen klar strukturierte Prozesse, deren Wirkungen einzelnen Verantwortlichen zuzurechnen sind.
- die zu beurteilenden Handlungen nur Einzelfälle betreffen. Soweit der Umgang mit den Daten bekannt oder aufklärbar ist und die Zusammenhänge und Verantwortlichkeiten durchschaubar sind, können der Betroffene oder die Datenschutzaufsicht sich auf das Ereignis konzentrieren und ihre Kontrollrechte geltend machen.

In solchen Konstellationen wird allgegenwärtiges Rechnen die Möglichkeiten der Interessendurchsetzung zwischen den Beteiligten verschieben und für die Datenverarbeiter auch neue Missbrauchsmöglichkeiten eröffnen. Dennoch entsprechen die neuen Problemstellungen dem »Erwartungshorizont« des Datenschutzrechts und es ist weiterhin möglich, die rechtliche Erlaubnis einer Datenverwendung zu überprüfen und datenschutzrechtliche Grundsätze wie Transparenz für den Betroffenen sowie Zweckbindung und Erforderlichkeit der Datenverarbeitung zur Anwendung zu bringen.[59] Einige Beispiele sollen dies belegen:

Findet allgegenwärtige Datenverarbeitung im *Arbeitsverhältnis* Anwendung, können die allgemeinen Zulässigkeitsregelungen zur Anwendung gebracht werden.[60] Die Verarbeitung personenbezogener Daten in einem Arbeitsverhältnis ist grundsätzlich nur dann zulässig, wenn zwei Voraussetzungen gegeben sind. Betriebsverfassungsrechtlich muss, sofern in dem Betrieb ein Betriebsrat besteht,[61] eine Betriebsvereinbarung gegeben sein und datenschutzrechtlich ein Erlaubnistatbestand. Sofern in einem Betrieb kein Betriebsrat besteht, ist allein die datenschutzrechtliche Zulässigkeit der Datenverarbeitung maßgeblich. Wenn eine wirksame Betriebsvereinbarung hinsichtlich der Datenverarbeitung gegeben ist, so erfüllt diese gleichzeitig die zweite Anforderung. Denn gemäß § 4 Abs. 1 BDSG kann sich eine Erlaubnis zur Datenverarbeitung aus dem Bundesdatenschutzgesetz selbst oder aus einer anderen Rechtsvorschrift ergeben. Im Arbeitsverhältnis praktisch relevante »andere Rechtsvorschriften« sind

[58] Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 57 ff., sowie die im Folgenden zu RFID genannte Literatur.

[59] Die datenschutzrechtlichen Untersuchungen zu RFID – s. z.B. Artikel-29-Datenschutzgruppe 2005a; Holznagel/Bonnekoh 2006, 21 ff.; Holznagel/Bonnekoh, MMR 2006, 17 ff.; Conrad, CR 2005, 537; Eisenberg/Puschke/Singelnstein, ZRP 2005, 9 ff.; Müller, DuD 2004, 215 ff.; Huber, MMR 2006, 728; Toutziaraki, DuD 2007, 107 ff.; Westerholt/Döring, CR 2004, 710 ff.; Bundesregierung, BT-Drs. 15/3190; für die USA Schmidt 2005, 193 ff. – beschränken sich auf solche übersichtlichen Verhältnisse; dies gilt auch für den rechtlichen Teil von Untersuchungen, die sich über RFID hinaus auf Ubiquitous Computing beziehen, s. z.B. Möller/Bizer, in TAUCIS 2006, 198 ff.

[60] S. z.B. Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 100 ff.

[61] Gemäß § 1 BetrVG werden in Betrieben mit in der Regel mindestens fünf ständigen wahlberechtigten Arbeitnehmern, von denen drei wählbar sind, Betriebsräte gewählt.

vor allem Tarifverträge und Betriebsvereinbarungen,[62] da sie die ansonsten gegebenenfalls von jedem einzelnen Mitarbeiter erforderliche Einwilligung in die Datenverarbeitungsvorgänge entbehrlich machen. Gemäß § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat bei der »Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen« mitzubestimmen. Für die »Bestimmung« reicht die objektive Möglichkeit der Überwachung aus. Sie muss nicht die primäre Zielsetzung des Arbeitgebers sein.[63] Dies ist bei Anwendungen allgegenwärtiger Datenverarbeitung in der Regel anzunehmen.

Da ohnehin eine Betriebsvereinbarung notwendig ist, kann bei deren Vereinbarung die datenschutzrechtliche Gestaltung der Anwendung geregelt werden. Hierbei können vor allem Maßnahmen zum System- und Selbstdatenschutz sowie zur Datensparsamkeit vereinbart werden.[64] Außerdem können Zweckänderungen der gewonnenen Daten ausgeschlossen werden. Eine heimliche Einführung und verdeckte Nutzung der Anwendung ist durch den Zwang zur Betriebsvereinbarung ausgeschlossen. Da die Betriebsvereinbarung ohnehin im Betrieb bekannt gemacht werden muss, kann bei dieser Gelegenheit auch eine ausführliche Erläuterung zu Zielsetzung und Funktionsweise der Anwendung veröffentlicht werden. Hierdurch kann für alle Interessierten eine ausreichende datenschutzrechtliche Transparenz gewährleistet werden. Betroffene haben die Möglichkeit, gegenüber ihrem Arbeitgeber arbeits- und datenschutzrechtliche Auskunft- und Korrekturrechte geltend zu machen.

Auch im *Versicherungsverhältnis* können die allgemeinen datenschutzrechtlichen Regelungen zur Anwendung kommen, wenn

[62] Tarifverträge und Betriebsvereinbarungen fallen unter den weit auszulegenden Begriff der »anderen Rechtsvorschriften« im Sinn des § 4 Abs. 1 BDSG.

[63] S. BAG, AP Nr. 2 zu § 87 BetrVG 1972, seither ständige Rechtsprechung.

[64] Die Zielsetzung allgegenwärtiger Datenverarbeitung und des Datenschutzrechts widersprechen sich weitgehend. Daher werden auch im Rahmen von Betriebsvereinbarung Lösungen sehr schwierig sein.

dort etwa Techniken allgegenwärtiger Datenverarbeitung eingesetzt werden sollen, um Modelle des Pay-per-Risk zu realisieren. Angenommen der Versicherungsnehmer soll sich vertraglich verpflichten, in regelmäßigen Abständen Protokolldaten aus seinem Auto an die Versicherung zu übermitteln, so ist dafür entweder nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG eine vertragliche Vereinbarung oder aber eine gesonderte schriftliche Einwilligung nach § 4a Abs. 1 BDSG notwendig.[65]

Ein entsprechender Versicherungsvertrag würde nicht gegen die Pflicht, eine Haftpflichtversicherung abzuschließen, und auch nicht gegen den Kontrahierungszwang der Versicherung nach § 5 Abs. 2 Pflichtversicherungsgesetz verstoßen. In diesem Gesetz sind keine inhaltlichen Grenzen hinsichtlich der Tarifgestaltung oder der Höhe der Versicherungsprämie enthalten. Insofern findet eine Regulierung allein durch die freie Vertragsgestaltung beider Seiten statt. Der Versicherungsnehmer ist insofern zwar gesetzlich verpflichtet, eine Kfz-Haftpflichtversicherung für sein Fahrzeug abzuschließen und aufrechtzuerhalten, es steht ihm aber frei, die Versicherungsgesellschaft zu wechseln, wenn er mit den Vertragsbedingungen nicht einverstanden ist.

Eine entsprechende Einwilligung wäre ebenfalls zulässig. Gibt jemand die Einwilligung zur Verarbeitung seiner personenbezogenen Daten, um in den Genuss der günstigeren Prämien zu kommen und so Geld zu sparen, besteht an der Freiwilligkeit der Einwilligung – von Extremen abgesehen – kein Zweifel.

Vor Abschluss des Vertrags oder vor Abgabe der Einwilligung muss die Versicherung den Versicherungsnehmer ausreichend über den Zweck der Datenübermittlung und die weitere Verarbeitung und Nutzung der Daten unterrichten. Ein heimliches Auslesen der Daten ist nicht möglich, da der Versicherungsnehmer erst die Sensoren einbauen oder die Übermittlung durchführen oder zum Abruf frei schalten lassen muss. Der Versicherungs-

[65] S. hierzu Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 131f.

nehmer kennt den Datenverarbeiter und kann ihm gegenüber seine Auskunfts- und Korrekturrechte geltend machen.

Ebenso sind Anwendungen allgegenwärtiger Datenverarbeitung in einem *Mietverhältnis* datenschutzrechtlich zu bewerten. Bietet der Vermieter eine Wohnung mit Sensoren zur Steuerung von Heizung, Klima, Licht und anderen Infrastrukturleistungen an, so hat er den Mieter hierüber umfassend zu unterrichten und dies ausdrücklich als gewünschten Teil der Vermieterleistungen in den Mietvertrag aufzunehmen oder den Mieter um eine Einwilligung zu bitten. Schließt der Mieter einen solchen Mietvertrag ab oder erteilt er schriftlich seine Einwilligung, ist grundsätzlich an der Freiwilligkeit seiner Willenserklärungen nicht zu zweifeln. Die Nutzung der Techniken allgegenwärtiger Datenverarbeitung ist damit gerechtfertigt. Der Mieter kann jederzeit seine Auskunfts- und Korrekturrechte geltend machen.

Im Rahmen eines Mietverhältnisses begibt sich der Mieter zwar in die Räume, die der Vermieter technisch ausgestattet hat und für die er den Betrieb der allgegenwärtigen Datenverarbeitung kontrolliert. Die Sensoren sind vermutlich unsichtbar in die Räume integriert. Daher besteht grundsätzlich eine Möglichkeit des Vermieters, Überwachungsdaten über das Verhalten des Mieters heimlich zu erheben. Da aber der Mieter über das Vorhandensein und die Funktionsweise der Sensoren unterrichtet worden ist und er jederzeit auf die Sensoren in den von ihm gemieteten Räumen faktisch zugreifen kann und ebenso jederzeit Auskunft vom Vermieter über die erhobenen Daten fordern kann, dürften seine Interessen weitgehend gewahrt sein. Er kann außerdem Löschung nicht mehr erforderlicher Daten verlangen.

In solchen Beispielen[66] mit übersichtlicher Technik und klarer Verantwortungsstruktur ist das Anknüpfen an »Verantwortungsräume«[67] nicht erforderlich. Sofern es einen Betreiber des Hintergrundsystems gibt,[68] in dem die von RFID-Tags oder Sensoren gewonnenen Daten verarbeitet werden,[69] ist er ohnehin die verantwortliche Stelle, unabhängig davon, ob er für einen »Raum« verantwortlich ist.

Soweit jedoch in den Räumen des »Verantwortlichen« andere Personen mit Techniken der allgegenwärtigen Datenverarbeitung personenbezogene Daten erheben, wird er nicht dadurch zur verantwortlichen Stelle, dass ihm etwa das Hausrecht zusteht. Selbst wenn er anderen Personen die Erhebung von Daten gestattet, treffen ihn dadurch keine datenschutzrechtlichen Pflichten.

Auch als Vermieter ist er nicht dafür verantwortlich, dass der Mieter oder ein anderer Nutzungsberechtigter nicht gegen datenschutzrechtliche Vorschriften verstößt.[70] Ihn treffen allenfalls in ganz bestimmten Konstellationen, in denen er für die Betroffenen eine Fürsorgepflicht hat und in denen er »das Aufstellen von Lesegeräten oder Sensoren vornehmen lässt oder duldet«,[71] eine Pflicht, diese spezifischen Betroffenen vor unzulässiger Datenerhebung zu schützen.[72] Diesen Anspruch müsste ein Betroffener gegen den Inhaber des Hausrechts gerichtlich geltend machen und dabei die gesamte Beweislast für das Vorliegen aller

66 Zur RFID-Datenverarbeitung im Einkaufsbeispiel s. näher Artikel-29-Datenschutzgruppe 2005a, 11; Westerholt/Döring, CR 2004, 711 ff.; Holznagel/Bonnekoh 2006, 21 ff.; Holznagel/Bonnekoh, MMR 2006, 17 ff.

67 S. hierzu Möller/Bizer, in TAUCIS 2006, 221 ff.

68 Als Beispiele werden der Betreiber eines UC-Hauses, der Eigentümer eines UC-Kraftfahrzeugs und der Betreiber eines Geschäfts in einer UC-Einkaufsmeile genannt.

69 Auf diesen Fall beschränken sich die Überlegungen zu den »Verantwortungsräumen«.

70 Auch die von Möller/Bizer, in TAUCIS 2006, 223, angeführte »rechtliche Verantwortung des Inhabers des Hausrechts« begründet keine datenschutzrechtlichen Pflichten, die den Inhaber ergänzend oder anstelle der verantwortlichen Stelle treffen.

71 Möller/Bizer, in TAUCIS 2006, 223.

72 Ob die informationelle Selbstbestimmung überhaupt unter die Schutzgüter des § 823 Abs. 1 BGB fällt, ist umstritten – s. z.B. mit Einschränkungen BGH, NJW 2003, 765; OLG Köln K&R 2002, 427f. dafür; dagegen z.B. Simitis, in: Simitis 2006, Einleitung Rn. 26 m.w.N.; Hager, in: Staudinger 2004, § 823 Rn. C 173. § 823 Abs. 2 BGB kommt als Anspruchsrundlage nicht in Frage, weil der »Raumverantwortliche« nicht gegen datenschutzrechtliche Vorschriften verstößt.

Anspruchsvoraussetzungen tragen – eine Methode des Grundrechtsschutzes, die nicht sehr praxisnah ist.

Die künftig praxisrelevanten Fälle, dass viele Spaziergänger in einer Einkaufs-Mall, die Reisenden in einem Bahnhof, die Besucher eines großen Amts oder die Studierenden in der Mensa einer Universität[73] Techniken der allgegenwärtigen Datenverarbeitung mit sich führen und nutzen, dürfte keine datenschutzrechtlichen Verantwortungsräume schaffen, die den Mall-Betreiber, die Bundesbahn, die Behörde oder die Universität für deren Datenverarbeitung verantwortlich macht.[74]

3.3.2 Allgegenwärtige Datenverarbeitung in komplexen Strukturen

Allgegenwärtiges Rechnen schafft nicht nur neue Handlungsmöglichkeiten zur Interessendurchsetzung und zum Datenmissbrauch. Es verändert auch die Form der Interaktion des Menschen mit Informationstechnik grundsätzlich und schafft dadurch Verhältnisse in denen

- viele Beteiligte mit ständig wechselnden Rollen beteiligt sind,
- vielfältige Zwecke gleichzeitig verfolgt werden,
- Daten auch in privaten oder gemischt privat/geschäftlichen Kontexten verwendet werden,
- die Datenverarbeitung spontan von den Techniksystemen selbst organisiert wird,
- die Datenverarbeitung für den Betroffenen unbemerkt erfolgt und in ihren Wirkungen undurchschaubar ist.

Auf diese neuen Verhältnisse sind die Grundsätze des datenschutzrechtlichen Schutzprogramms kaum anwendbar. Die Ziele,

[73] S. hierzu die Szenarien 71 ff.

[74] Dies konstatieren selbst Möller/Bizer, in TAUCIS 2006, 223, für den »Betrieb mobiler Lesegeräte bzw. Sensoren durch Dritte«, der vom Inhaber des Hausrechts nicht festzustellen ist.

die mit dem Einsatz allgegenwärtiger Datenverarbeitung verfolgt werden, widersprechen den Zielen, die mit den Prinzipien des Datenschutzrechts verfolgt werden. Im Konflikt zwischen beiden dürfte entscheidend sein, dass die Anwendungen der allgegenwärtigen Datenverarbeitung den Betroffenen in den meisten Fällen nicht aufgedrängt – in diesem Fall dürften die Datenschutzprinzipien greifen –,[75] sondern von diesen gewollt werden. Sie wollen sich mit ihrer Hilfe die Träume erfüllen, die mit allgegenwärtigem Rechnen verbunden sind.[76] Sie werden dann als Konsequenz auch damit einverstanden sein müssen, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweise, Gewohnheiten, Einstellungen und Präferenzen erhalten. In diesen neuen Verhältnissen wird das bisherige Schutzprogramm als solches in jedem seiner Bestandteile in Frage gestellt.

3.4 Grenzen normativen Datenschutzes

Auch in diesen dynamischen und komplexen Verhältnissen gelten die Datenschutzregelungen fort und sind weiterhin der Maßstab für rechtmäßiges Verhalten. Die Frage, die hier verfolgt werden soll, ist jedoch, welche Chancen zu ihrer Realisierung und Durchsetzung bestehen. Einfach davon auszugehen, dass sie beachtet werden, nur weil sie im Gesetz stehen, wäre naiv. Daher ist es wichtig zu fragen, ob diese Prinzipien in einer Welt der allgegenwärtigen Datenverarbeitung noch angemessen sind oder ob sie nur noch als unverständliche bürokratische Hemmnisse angesehen werden, den meisten Menschen unbekannt bleiben oder einfach ignoriert werden.

[75] S. oben 120 ff.

[76] S. oben 13 ff. (1.1).

3.4.1 Verantwortlichkeit

Verantwortlich für die Einhaltung der Datenschutzregeln ist die »verantwortliche Stelle«. Dies ist nach § 3 Nr. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Verantwortliche Stelle kann sowohl eine natürliche Person sein als auch ein Unternehmen oder eine Behörde.[77]

Kein Problem, die verantwortliche Stelle festzustellen, besteht, wenn der Betreiber in seinem Supermarkt Ubiquitous Computing einsetzt, ein Vermieter sein modernes Büro- oder Wohnhaus mit Ubiquitous Computing ausstattet oder ein Produktionsbetrieb seine Teil- und Endprodukte oder eine Behörde ihre Akten mit RFID-Tags versieht.[78] In solch einfach strukturierten Konstellationen können die Kontrollstelle oder der Betroffene sofort erkennen, wer für die rechtmäßige Verarbeitung personenbezogener Daten verantwortlich ist. Sind zwei oder mehr Stellen an der Datenverarbeitung beteiligt, teilen sie sich die Verantwortung oder sind gemeinsam verantwortlich.[79]

Ein spezifisches Problem allgegenwärtiger Datenverarbeitung, Verantwortung zu umgehen, kann auch in solch einfach strukturierten Verhältnissen entstehen, wenn derjenige, der etwa RFID- oder Sensordaten aufnimmt, diese ins Ausland transferiert. Solange er nicht in der Lage ist, sie einer Person zuzuordnen, kann er dies ohne Verstoß gegen Datenschutzrecht tun. Wird erst dort von anderen der Personenbezug durch die Kombination mit anderen Datenbeständen – etwa im Weg eines Data Mining – hergestellt, unterliegen diese personenbezogenen Daten nicht mehr deutschen oder europäischen Rechtmäßigkeitsmaßstäben.[80]

[77] S. hierzu Wedde in: Roßnagel 2003a, 528 ff.

[78] S. oben 120 ff.

[79] Dass die Feststellung des Verantwortlichen und die Durchsetzung von Kontroll- oder Betroffenenrechten praktisch schwierig sein können, ist kein spezifisches Problem allgegenwärtiger Datenverarbeitung.

[80] S. zu diesem Problem auch Möller/Bizer, in: TAUCIS 2006, 201 f.

Unter den Bedingungen allgegenwärtiger Datenverarbeitung werden grundsätzlich die schiere Menge der personenbezogenen Daten, die Vielzahl der beteiligten Akteure, die spontane Ver- und Entnetzung sowie der ständige Rollenwechsel zwischen Datenverarbeiter und Betroffenen[81] zu einer Zersplitterung der Verantwortlichkeit für die datenverarbeitenden Vorgänge führen und es erheblich erschweren, diese zu kontrollieren.[82] Zu vielen Anwendungen tragen unter Umständen sehr viele indirekt miteinander vernetzte Objekte, Dienste und Institutionen bei, die für sich genommen kaum für den Gesamtvorgang verantwortlich gemacht werden können und erst in ihrem Zusammenwirken den äußerlich wahrnehmbaren Effekt bewirken. Die Problematik der »Dissipation der Verantwortung« dürfte mit Ubiquitous Computing stark an Bedeutung gewinnen.[83]

Ein Problem, den Verantwortlichen festzustellen, kann sich bei Anwendungen allgegenwärtiger Datenverarbeitung ergeben, wenn »Infrastrukturen« entstehen und vergehen oder wenn sie vielen Nutzern ohne Anmeldung zur Verfügung stehen. Neuartige Fragen können sich in dieser Hinsicht etwa für Ad-Hoc-Netze stellen, die sich kurzfristig aus den Autos in einem Stau bilden, oder für Sensornetze, die grundsätzlich jeder als Informationsquelle nutzen kann. In solchen Fällen kann es schwierig bis unmöglich sein festzustellen, wer Daten erhoben und verarbeitet hat, und zu verfolgen, wohin die Daten gelangt sind.

Dies gilt zum Beispiel für Kommunikationsnetze ohne feste Infrastruktur, in denen die Kommunikationsverbindungen durch Peer-to-Peer-Kontakte ermöglicht werden, die sich ad hoc mit zufälligen Beteiligten bilden und in denen jeder Teilnehmer ständig wechselnd die Rolle des Senders und des Empfängers und

[81] Dadurch wird eine Vielzahl von Personen sowohl Betroffener als auch Verantwortlicher von personenbezogener Datenverarbeitung sein.

[82] S. Roßnagel/Pfitzmann/Garstka 2001, 22 ff., 185 f.; Mattern 2005a, 26 f.; Möller/Bizer, in: TAUCIS 2006, 119.

[83] Mattern 2005a, 23.

Vermittlers übernimmt.[84] Er verarbeitet für die Telekommunikationsverbindung personenbezogene Verkehrs-, Nutzungs- und Inhaltsdaten, die er zur Kenntnis nehmen könnte, aber an denen er kein Interesse hat, und die er nur verarbeitet, um an dem Netz teilnehmen zu können. Er ist kein Anbieter von Telekommunikationsdiensten im Sinn des § 3 Nr. 24 TKG, weil er nicht einen Dienst in der Regel gegen Entgelt anbietet, der in der Übertragung von Signalen über Telekommunikationsnetze besteht, sondern weil er nur gelegentlich, zeitweilig und eher zufällig an der Herstellung von Telekommunikationsverbindungen ohne spezifisches Telekommunikationsnetz mitwirkt.[85] Ebenso wenig bietet er Telemediendienste an. Er ist daher auch kein Adressat der Datenschutzregelungen des Telekommunikationsgesetzes und des Telemediengesetzes. Dennoch müssten auch für ihn die Grundsätze der Zweckbindung, der Erforderlichkeit und des Telekommunikationsgeheimnisses gelten. Für diese Formen der Kommunikation besteht eine Regelungslücke.[86]

Auch aufgrund der Komplexität der Datenerhebungs- und -verarbeitungsvorgänge dürfte die »Zurechenbarkeit« Probleme bereiten. Oft wird es nicht möglich sein, von jeder in einem IT-System ausgeführten Aktion während ihres Ablaufs und danach festzustellen, wem diese Aktion zuzuordnen ist und wer sie letztlich zu verantworten hat.[87] Abgesehen davon, dass durch das Nachhalten der Verantwortlichkeit oft personenbezogene Daten erhoben und gespeichert werden müssen, ist dies in einer Welt, in der Kommunikations- und Dienstbeziehungen oft nur spontan und kurz eingegangen werden und kommunikationsfähige Alltagsdinge gewissermaßen selbst nicht genau wissen, wieso sie bezogen auf den konkreten Kontext ein spezifisches Verhalten aufweisen, ein schwieriges Unterfangen.[88]

[84] S. hierzu Herrtwich 2003, 75f.

[85] S. z.B. Herrtwich 2003, 75f.

[86] S. hierzu Roßnagel, NVZ 2006, 281 ff.; Roßnagel 2006, 150.

[87] Dierstein, Informatik-Spektrum 2004, 343 ff.

[88] Mattern 2007a, 22.

Probleme der datenschutzrechtlichen Verantwortung ergeben sich weiterhin, soweit die Geltung des Datenschutzrechts ausgeschlossen ist. Dies gilt nach §§ 1 Abs. 2 Nr. 3 und 27 Abs. 1 Satz 2 BDSG vor allem für die Erhebung, Verarbeitung und Nutzung von Daten, die »ausschließlich für persönliche oder familiäre Tätigkeiten« erfolgt. Eine solche rein private Datenverarbeitung liegt vor, wenn natürliche Personen lediglich Daten über sich oder für sich speichern und diese nur für den persönlichen Gebrauch verarbeiten oder nutzen.[89] Gemeint ist damit etwa das private Adressverzeichnis, die Sammlung der Briefentwürfe, das persönliche E-Mail-Verzeichnis, die persönliche Link-Liste oder das private elektronische Foto-Album. Diese privaten oder familiären Datensammlungen sollten gegenüber den Anforderungen des Datenschutzes privilegiert werden, weil diese für sie als unverhältnismäßig empfunden werden. Etwas anderes gilt jedoch, wenn personenbezogene Daten den rein privaten Bereich verlassen, indem sie etwa auf einer privaten Homepage Dritten zugänglich gemacht werden[90] oder indem sie für berufliche oder gewerbliche Zwecke oder geschäftsmäßig verarbeitet oder genutzt werden.[91] Dieser rechtliche Freiraum lässt jedoch einen großen Spielraum für den Einsatz allgegenwärtiger Datenverarbeitung, ohne dass hierfür das Datenschutzrecht gilt.[92]

Die Privilegierung gilt auch, wenn der Einzelne allgegenwärtige Datenverarbeitung zur Erweiterung seiner Sinne benutzt. Nicht

[89] S. Wedde, in: Roßnagel 2003a, 534; Gola/Schomerus 2006, § 1 Rn. 21; Dammann, in: Simitis 2006, § 1 Rn. 147 ff.; die Privilegierung gilt für natürliche Personen, s. Art. 3 Abs. 2 DSRL, zu weitgehend Bergmann/Möhrle/Herb, § 1 Rn. 37, die hieraus eine entsprechende Privilegierung für datenverarbeitende Stellen ableiten, die ideelle, karitative, gemeinnützige oder mildtätige Zwecke verfolgen; ähnlich auch Schaffland/Wiltfang, § 1 Rn. 22.

[90] S. EuGH, MMR 2004, 95 ff. mit einer Anmerkung von Roßnagel.

[91] S. hierzu Wedde, in: Roßnagel 2003, 534; Gola/Schomerus , § 27 Rn. 12; Simitis, in: Simitis 2006, § 27 Rn. 47.

[92] Ansprüche auf Löschung und Unterlassung und im Extremfall auf Schadensersatz könnten sich eventuell aus § 823/1004 BGB ergeben. Für einen Prozess, in dem diese Rechte geltend zu machen sind, hat der Betroffene die volle Beweislast für Sorgfaltspflichtverletzung, Kausalität und Verschulden.

dem Datenschutzrecht unterfallen danach etwa alle Daten, die er nicht für geschäftliche Zwecke rund um die Uhr durch seine Sensoren erhebt. So kann er auch eine Scheibe in seinem Haus nutzen, die ihm immer anzeigt, welche Nachbarn in der letzten Stunde vorbeigegangen sind.[93] Dies gilt ebenso für alles, was das eigene Kraftfahrzeug an Umgebungsinformationen aufnimmt. Ausgenommen von datenschutzrechtlichen Vorgaben sind auch alle persönlichen und familiären Lokationsdaten, die von Gegenständen im privaten Eigentum des Nutzers aufgenommen werden, auch wenn dadurch indirekt Daten über Dritte erhoben werden. Schließlich muss es zur privaten Datenverarbeitung gezählt werden, wenn der Nutzer sich etwa mit der Kommunikationskapazität seines Kraftfahrzeugs an Ad-Hoc-Netzen beteiligt.

Unter die Ausnahmen fallen auch alle Daten, die der Nutzer zu privaten Zwecken gespeichert hat und ihm zur Erweiterung seines Gedächtnisses wiedergegeben werden. Nicht erfasst sind daher sogar die Aufnahme und Speicherung aller Umgebungsinformationen durch eine Person, die sich ihr privates Tagebuch in Form von Bild- und Tonaufnahmen aller Ereignisse erstellt, die sich für sie den Tag über ereignen. Kein Thema des Datenschutzes sind Bilder, Namen, Funktionsdaten und Profile von Personen, die man wieder erkennen oder mit denen man problemlos Themen der Unterhaltung finden will. Dies gilt ebenso für alle Aufnahmen von Umgebungsinformationen, die man zu Beweiszwecken speichert oder um sich erinnern zu können, was wer wann getan hat. Schließlich fällt auch das »Gedächtnis« aller privaten Dinge aus der Geltung des Datenschutzrechts heraus.

Nur privaten oder familiären Zwecken dienen auch alle Geräte, die für die Entlastung von Arbeitsaufgaben im persönlichen oder familiären Umfeld genutzt werden. Dies gilt zum Beispiel für alle Anwendungen allgegenwärtiger Datenverarbeitung im Wohnhaus oder im Garten. Werden durch die Sensoren in der Wohnung auch Gäste oder Nachbarn erfasst, fällt dies nicht unter das Datenschutzrecht.

[93] Dieses Beispiel stammt von Mark Weiser, s. Sietmann, c't 2004/16, 88.

Nicht anders ist es zu beurteilen, wenn allgegenwärtige Datenverarbeitung benutzt wird, um einen virtuellen Sicherheitsgürtel um die eigene Person, um die Kinder oder um Haus und Hof zu legen. Privilegiert sind daher alle Anwendungen des Wearable Computing, die der Sicherheit der jeweiligen Person dienen, oder eines sensorgestützten Haussicherungssystems, das jede Bewegung rund ums Eigenheim registriert.

3.4.2 Transparenz

Der Grundsatz der Transparenz fordert, die Daten grundsätzlich bei dem Betroffenen zu erheben und ihn zuvor zu unterrichten. Bei jeder neuen Speicherung ist er zu benachrichtigen. Gegenüber der verantwortlichen Stelle hat er Auskunftsrechte.

Die bisherigen Instrumente der Transparenz stoßen jedoch künftig 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.[94] Die Unsichtbarkeit der Erfassung ist ein Design-Merkmal der Technik und insofern kein behebbarer Fehler.[95] Kommunikationsfähige Gegenstände und sensorbestückte Umgebungen sind fast immer aktiv und erheben eine Unmenge Daten. Die Betroffenen wissen aber nie, ob und wenn ja welche Handlungen von ihnen beobachtet und registriert werden und welche Datensammlungen zusammengeführt werden.[96] Es fehlt an besonderen Anlässen und Momenten, die bisher eine Da-

[94] S. auch Roßnagel/Müller, CR 2004, 628f.; Langheinrich 2005a, 337f.; Mattern 2003c, 32; Möller/Bizer, in: TAUCIS 2006, 204.

[95] S. Möller/Bizer, in: TAUCIS 2006, 208.

[96] Mattern 2004, 328; Mattern 2005a, 16.

tenerhebung begründen und rechtfertigen.[97] Niemand würde es akzeptieren, wenn er täglich tausendfach bei meist alltäglichen Verrichtungen Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Würde das Recht dennoch auf solchen Zwangsinformationen bestehen, würde es das Gegenteil von Aufmerksamkeit und Sensibilität erreichen.[98]

Selbst wenn der Betroffene dies wollte, stehen bei den datenverarbeitenden Alltagsgegenständen – anders als bei der Internetkommunikation – keine oder keine adäquaten Ausgabemedien zur Verfügung. Für einen Teil der möglichen Anwendungen ist vorstellbar, auf Ausgabemedien anderer Artefakte wie etwa die Anzeige auf einem PDA oder den Lautsprecher im Ohrring zurückzugreifen. Gleichwohl werden oft keine Ausgabemedien mit ausreichend großer visueller Darstellungsfläche, Übermittelungsbandbreite oder Adaption an die Umgebungsbedingungen zur Verfügung stehen.[99]

Eine allgemeine Kennzeichnungspflicht für Sensoren und Lesegeräte wäre in bestimmten Fällen möglich – etwa am Eingang eines Verkaufslokals oder eines öffentlichen Gebäudes.[100] Damit würde zwar über die Möglichkeit einer Datenerhebung informiert. Ob eine solche im Einzelfall aber stattfindet und welche Daten erfasst werden, kann der Betroffene einem derartigen allgemeinen Hinweis nicht entnehmen. Eine Kennzeichnungspflicht

97 S. hierzu oben 115 ff.

98 S. zum Aufmerksamkeitsproblem auch Möller/Bizer, in: TAUCIS 2006, 208. Dennoch fordern sie von den Betreibern eines Hintergrundsystems umfassende Unterrichtung aller Betroffenen – Möller/Bizer, in: TAUCIS 2006, 225, 235; die von der Artikel-29-Datenschutzgruppe 2005a, 15f. geforderten Piktogramme und Hinweise auf RFID-Chips sind nur hilfreich, solange nicht (beinahe) jeder Gegenstand einen solchen trägt. Ab dem Jahr 2010 werden jährlich mehr als 500 Milliarden RFID-Tags in Umlauf gebracht werden – s. UNESCO 2007, 45.

99 Roßnagel/Müller, CR 2004, 629.

100 Die Transparenzpflichten nach § 6c BDSG gelten nicht für das Auslesen von RFID-Chips – s. Hornung, MMR 5/2006, XX ff., und die Transparenzanforderungen nach § 6b BDSG gelten nicht für Sensoren.

würde dem Transparenzdefizit also nur in Einzelfällen abhelfen können.[101]

Außerdem setzen hohe Komplexität und vielfältige Zwecke der möglichen Transparenz objektive Grenzen.[102] Für viele Anwendungen wird bei Datenerhebung unklar sein, ob die Daten personenbezogen sind.[103] Sie erhalten den Personenbezug – wenn überhaupt – oft viel später. Eine einzelne Erhebung mag irrelevant erscheinen, besondere Bedeutung wird sie oft erst dadurch erlangen, dass sie nachträglich mit vielen anderen Daten zusammengeführt wird. Dann besteht aber keine Möglichkeit mehr, den Betroffenen zu benachrichtigen. Für andere Anwendungen kann der Zweck der Datenverarbeitung mehrfach wechseln und sich auch unvorhergesehen einstellen. Vielfach wird eine unerwünschte (Mit-)Erhebung durch die mobilen Geräte anderer Kooperationspartner erfolgen. Viele Anwendungen werden ineinander greifen und verteilte Ressourcen nutzen (z.B. Mitnutzung des Ausgabemediums eines anderen Gegenstands). Andere Anwendungen müssen zu ihrer Funktionserfüllung benötigte Daten austauschen (z.B. Ereignisdienst braucht externe Information über Ereigniseintritt). Eine Erhebung beim Betroffenen und erst recht seine Unterrichtung über die zu erhebenden Daten und den Zweck ihrer Verarbeitung wird daher vielfach unmöglich oder sehr schwierig sein.

Sensornetze, zu denen sich benachbarte Sensoren drahtlos spontan vernetzen, in denen die Sensoren ihre Arbeit untereinander abstimmen und relevante Daten austauschen, ermöglichen eine flexible und nahezu unsichtbare Beobachtung der Umwelt.[104] Die einzelne Datenerhebung ist weitgehend irrelevant, sie kann auch nicht im Einzelfall angezeigt werden. Eine nachträgliche Auskunft über alle verarbeiteten Daten ist prinzipiell möglich, würde aber eine Speicherung aller erhobenen und verarbeiteten

101 S. Möller/Bizer, in: TAUCIS 2006, 208.

102 S. Roßnagel/Müller, CR 2004, 629.

103 S. oben 91 ff.

104 S. z.B. Mattern 2005a, 15.

Daten voraussetzen, um im Ausnahmefall eines Auskunftsbegehrens die Daten des Anfragenden herausdestillieren zu können.[105] Dies ist weder praktisch möglich noch datenschutzrechtlich gewollt.[106]

Wenn das Prinzip der Transparenz nicht aufgegeben werden soll, bedarf es angepasster Konzepte, um bei den Betroffenen das Wissen um die Datenverarbeitung zu ermöglichen. Statt Zwangsinformationen über hunderte einzelner Verarbeitungsvorgänge täglich, sollte die Transparenz vor allem auf Strukturinformationen über Datenverarbeitungssysteme zielen und das Informationsinteresse des Betroffenen dann befriedigen, wenn er dies wünscht.[107]

3.4.3 Einwilligung

Eine Einwilligung in die Verwendung oder Nutzung personenbezogener Daten ist der genuine Ausdruck informationeller Selbstbestimmung. Sie gibt der verantwortlichen Stelle die Erlaubnis, die Daten des Einwilligenden für den in der Einwilligung genannten Zweck zu erheben, zu verarbeiten oder zu nutzen. Um wirksam zu sein, muss sie freiwillig und formgerecht, auf der Grundlage einer ausreichenden Unterrichtung und unter eindeutiger Bezeichnung des spezifischen Zwecks erteilt werden. Für einen neuen Zweck ist immer auch eine neue Einwilligung notwendig.

In der Welt allgegenwärtiger Datenverarbeitung eine Einwilligung jedoch für jeden Akt der Erhebung, Verarbeitung und Nutzung zu fordern, würde angesichts der Fülle und Vielfalt der Vorgänge und der Unzahl von verantwortlichen Stellen zu einer

[105] S. hierzu auch weiter unten 150.

[106] Probleme der Unterrichtung sehen auch Möller/Bizer, in: TAUCIS 2006, 208.

[107] S. Roßnagel/Pfitzmann/Garstka 2001, 171f.; Roßnagel/Müller, CR 2004, 629.

Überforderung aller Beteiligten führen.[108] Nur in seltenen Fällen wird es für die verantwortliche Stelle tatsächlich möglich sein, ein Einwilligungsmanagement in der Weise zu betreiben, dass sie alle Betroffenen für jede Datenverarbeitung anspricht, informiert und um ihre Einwilligung bittet.[109]

Noch weniger umsetzbar wäre es, für die Einwilligung die geltenden Formvorschriften – Schriftform oder elektronische Form – zu fordern. Selbst eine Einwilligung in der für das Internet gedachten Form des § 13 Abs. 2 TMG[110] dürfte unter den Umständen ständiger und verteilter Datenverarbeitung meist unpraktikabel sein. Angesichts der potentiell riesigen Zahl von impliziten (Mini-)Interaktionen und der ebenso großen Bandbreite an Nutzerschnittstellen scheint es nicht praktikabel, bekannte Verfahren wie beispielsweise einen Bestätigungs-Knopf oder gar eine Einwilligung durch elektronische Signatur allgemein einsetzen zu wollen.[111]

Ist allgegenwärtige Datenverarbeitung weit verbreitet, kann in vielen Fällen auch die Freiwilligkeit der Einwilligung fraglich sein. Dies ist insbesondere dann der Fall, wenn bestimmte Dienstleistungen oder Produkte für die Betroffenen, die derartige Datenverarbeitungen ablehnen, nicht mehr zur Verfügung stehen. [112]

Für das RFID-Umfeld wurde die Forderung erhoben, den Chip zu deaktivieren, wenn eine Einwilligung nicht möglich ist.[113] Sollte die Deaktivierung von der verantwortlichen Stelle gefordert werden, könnte auf dem gleichen Weg auch eine Einwilligung erteilt

[108] S. hierzu auch Roßnagel/Müller, CR 2004, 629, Langheinrich 2005a, 338f.; Möller/Bizer, in: TAUCIS 2006, 211.

[109] So aber Möller/Bizer, in: TAUCIS 2006, 206.

[110] S. zu dieser Roßnagel/Banzhaf/Grimm 2003, 162f.

[111] Langheinrich 2005a, 339.

[112] S. hierzu auch Möller/Bizer, in: TAUCIS 2006, 211, die daraus den einfachen Schluss ziehen, dass solche Anwendungen unzulässig sind.

[113] So die Forderung von Möller/Bizer, in: TAUCIS 2006, 206.

werden.[114] Die Deaktivierung durch den Betroffenen ist schon bei RFID-Anwendungen nicht immer eine geeignete Lösung, da sie die weitergehende Nutzung des Chips in der Sphäre des Betroffenen verhindert.[115] Diese Reaktionsweise ist aber keine Lösung bei anderen Anwendungen der allgegenwärtigen Datenverarbeitung, die zur Datenerfassung durch Sensoren, Lokalisatoren, biometrische Verfahren oder Kameras führt.

In der Welt allgegenwärtiger Datenverarbeitung wird die Einwilligung als Instrument des Datenschutzrechts in der bisher bekannten 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. Eine Renaissance könnte die Einwilligung – und damit die informationelle Selbstbestimmung – nur erleben, wenn sie eine Allianz mit der Datenschutztechnik eingeht.[116]

3.4.4 Zweckbindung

Die Zweckbindung soll dem Betroffenen ermöglichen, die Preisgabe von Daten entsprechend seiner sozialen Rolle im jeweiligen sozialen Kontext selbst zu steuern. Mit ihr ist ein Zugriff Unberechtigter auf die Daten, eine Datenverarbeitung auf Vorrat und die Bildung umfassender Profile nicht zu vereinbaren.[117]

Bei der Zweckbindung widerspricht bereits deren Ziel, die Datenverarbeitung zu steuern und auf den festgelegten Zweck zu

[114] Es würde sich dann also um ein einfach strukturiertes Verhältnis allgegenwärtiger Datenverarbeitung handeln – s. oben 120 ff. (3.3.1).

[115] S. z.B. Langheinrich 2007a, 135; Langheinrich 2005a, 355, Müller/Handy, DuD 2004, 658; Fabian, in: TAUCIS 2006, 267 – s. zur Sekundärnutzung oben 65 ff. (Logistik).

[116] S. Köhntopp 2001 und Nedden 2001 sowie weiter unten 176.

[117] S. BVerfGE 65, 1 (49); Scholz 2003, 1845 ff.

begrenzen, der Idee von Ubiquitous Computing, den Nutzer unbemerkt und spontan in komplexen Situationen technisch zu unterstützen. Je vielfältiger und umfassender die zu erfassenden Alltagshandlungen sind, umso schwieriger wird es, den Zweck einzelner Datenverarbeitungen vorab festzulegen und zu begrenzen.[118] Die klare Bestimmung des Zwecks, der oft durch die funktionale Zuordnung zu einem Gerät abgegrenzt war (zum Beispiel: Fernsprechapparat für Sprachkommunikation), ist in der Welt allgegenwärtiger Datenverarbeitung so nicht mehr möglich.

Daher stellt sich die Frage, ob der bereichsspezifisch, klar und präzise festgelegte Zweck, den das Bundesverfassungsgericht fordert,[119] noch das angemessene Kriterium sein kann, um die zulässige Datenverarbeitung abzugrenzen.[120] Soll etwa »Ad-Hoc-Kommunikation« als eine Form der Telekommunikation zugelassen werden, für die sich die Infrastruktur jeweils situationsabhängig und ständig wechselnd mit Hilfe der Endgeräte der Kommunikationspartner und unbeteiligter Dritter bildet,[121] kann nicht vorherbestimmt werden, welche Beteiligten zu welchen Zwecken welche Daten erhalten und verarbeiten. Jeder kann ein solches 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.

Sensornetze, die sich aus in die Umwelt eingebrachten Sensoren spontan bilden, sollen ihre Umwelt beobachten und flexibel für

[118] S. hierzu auch Roßnagel/Müller, CR 2004, 630; Langheinrich 2005a, 337; Mattern 2005a, 31.

[119] BVerfGE 65, 1 (44, 46).

[120] S. kritisch aus anderen Gründen Roßnagel/Pfitzmann/Garstka 2001, 29 ff.

[121] S. zu Ad-Hoc-Netzen auch Ernst 2005, 127 ff.

vielfältige Zwecke des Monitorings benutzt werden. Sie können etwa für die Beobachtung von Umweltbelastungen, Bewegungen, Materialveränderungen und viele andere Zwecke genutzt werden, ohne dass dies bei der Erhebung eines einzelnen Datums feststehen muss oder kann.[122]

Der eindeutige bestimmte Erhebungszweck wird bei Ubiquitous Computing oft nur noch schwer einzugrenzen sein. Statt auf künstliche Intelligenz setzt man auf eine möglichst exakte Erfassung des aktuellen Kontexts, um auch ohne echtes Verständnis der Situation eine angepasste Reaktion zu erhalten. Oder man versucht durch hohe Redundanz, auch in der Datenerhebung, technische Unzuverlässigkeiten, zum Beispiel beim Lesen von RFID-Tags, auszugleichen. Dieser Selbstzweck bei der Datenerhebung – das Sammeln von möglichst vielen Informationen, da später potentiell alles relevant sein kann – erschwert nicht nur die Zweckbindung, sondern erhöht gleichzeitig auch den Sammeleifer: Selbst scheinbar banale Daten können durch Computeranalyse mit relevanten Fakten korreliert werden.[123]

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. So kann zum Beispiel das eine Datum, dass ein Reisender einen Zugwaggon bestiegen hat, für die automatische Fahrscheinkontrolle, für das Reservierungssystem, das ihn zu seinem Platz geleiten soll, für das Bewirtungssystem, das ihm das bestellte Frühstück bringen soll, für das Bonussystem, das ihm automatisch »Meilen« gut schreibt, für das Telekommunikationssystem, das ihn am Platz mit seinen Telekommunikationszugängen versorgt, für das Reiseplanungssystem, das ihn im Zug lokalisiert und für viele weitere Systeme, die ihm während

[122] S. z.B. Mattern 2005a, 15.

[123] Langheinrich 2005a, 337.

der Zugreise noch weitere Dienstleistungen erbringen, benutzt werden. Alle diese Systeme können mit weiteren Systemen kooperieren, weitere Daten über den Reisenden besorgen oder Daten an die anderen Systeme abgeben. Für Anwendungen, die auf ein umfassenderes Verständnis von Vorgängen angewiesen sind, könnte zum Beispiel aus einer Vielzahl von Messgrößen, die von unterschiedlichen Stellen zu ihren jeweiligen Zwecken erhoben worden sind, anschließend ein Kontextverständnis für bestimmte Situationen oder Personen generiert werden. Dieses benötigt nicht nur die Zweckänderung aller genutzten Daten, aufgrund der Heterogenität und der großen Zahl der beteiligten Komponenten ist eine nachträgliche Kontrolle der Herkunft der Daten nicht mehr möglich.[124]

Sollen Anwendungen allgegenwärtiger Datenverarbeitung die Sinne des Nutzers erweitern, können sie nicht nur für einen bestimmten Zweck Daten erheben. Sie müssen wie die Sinne des Nutzers die gesamte Umwelt wahrnehmen. Erst wenn diese Daten erhoben und gespeichert sind, kann nach und nach eine zweckorientierte Auswahl und Bewertung erfolgen. Erst danach können die Ergebnisse der »Sinneseindrücke« gelöscht werden – es sei denn sie sollen der Möglichkeit dienen, sich an etwas zu erinnern. Selbst wenn ein Zweck bestimmt wird, kann dieser so umfassend sein, dass er die Erhebung und Speicherung vielfältiger und umfassender Daten erfordert. Soll allgegenwärtige Datenverarbeitung der Vorsorge für oder der Gewährleistung von Sicherheit dienen, kann es zum Beispiel erforderlich sein, alle Bewegungen um und in einem Gebäude zu erkennen und auszuwerten. Dies macht eine umfassende Datenerhebung und -verarbeitung in einem großen Bereich erforderlich.

Ähnliche Probleme ergeben sich mit dem Verbot einer Datenhaltung auf Vorrat. Wenn viele Anwendungen ineinander greifen, Daten aus anderen Anwendungen übernehmen und für den Nutzer Erinnerungsfunktionen für künftige Zwecke erfüllen

[124] BSI 2004, 109.

sollen, die noch nicht bestimmt werden können, sind Datenspeicherungen auf Vorrat nicht zu vermeiden.[125] Das Verbot der Vorratsspeicherung ist in einer Welt von sensorbestückten, kommunikationsfähigen Gegenständen, die sich an ihre »Erlebnisse« erinnern können und sollen, kaum mehr adäquat. Es würde das »Gedächtnis« der Gegenstände so gut wie verbieten. Gewünschte Anwendungen würden verhindert, die eine nachträgliche Rekonstruktion des Ortsbezugs oder eine episodische Erinnerung der Gegenstände voraussetzen. Der Traum der Nutzer, ihr Gedächtnis durch solche Techniken zu erweitern, würde dadurch zerstört. Eine zentrale Idee allgegenwärtiger Datenverarbeitung liegt aber gerade in der Speicherung von Daten für zukünftige, jedoch a priori unbekannte Zwecke.[126]

Wenn die Umgebungssysteme 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.[127] Wenn Geräte oder Dienstleistungen dem Nutzer Arbeit abnehmen sollen, müssen sie über seine Bedürfnisse, Vorlieben, Gewohnheiten und Pläne Bescheid wissen. Sie müssen vom Nutzer ein Profil bekommen oder es sich durch Beobachtung erarbeiten. Für Profile, die die informationelle Selbstbestimmung gefährden, und Profile, die eine optimale Befriedigung der Nutzerinteressen gewährleisten, bedarf es weiterer Unterscheidungskriterien, die nicht allein an der Tatsache einer Profilbildung anknüpfen können.[128]

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« in §§ 28 und 29 BDSG und Gebote zur Abwägung

[125] S. Mattern 2005a, 31.

[126] S. hierzu auch Mattern 2003c, 32.

[127] S. hierzu Schwenke 2006.

[128] S. hierzu für Location Based Services Jandt/Laue, K&R 2006, 316 ff.

mit »schutzwürdigen Interessen« des Betroffenen wären für die informationelle Selbstbestimmung kontraproduktiv, weil sie praktisch die Datenverarbeitung freigeben und für den Betroffenen unkontrollierbar machen.[129] Bleiben solche Generalklauseln bestehen, werden sie bei allgegenwärtiger 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. Die geforderte Abwägung mit den »schutzwürdigen Interessen« des Betroffenen wird hieran nichts ändern können, weil die verantwortliche Stelle diese Interessen nicht kennt und die Datenverarbeitung dem Betroffenen im Regelfall verborgen bleibt.

Mit der vielfältigen – oft unbewussten – Verfügbarkeit über personenbezogene Daten könnten sich faktisch neue Offenbarungspflichten ergeben, die zu einer nachträglichen Zweckänderung führen. Wenn die Dinge vieles um sie herum registrieren und speichern, könnte man durch Zusammenführung der gespeicherten Daten die Vergangenheit rekonstruieren und damit in vielen Fällen der Wahrheitsfindung dienen.[130] Soll in der Familie, im Wohnumfeld, am Arbeitsplatz, im Straßenverkehr,[131] im Rahmen der öffentlichen Sicherheit oder der gerichtlichen Beweisaufnahme geklärt werden, wie sich ein Ereignis zugetragen hat, könnte sich jeder verpflichtet fühlen oder verpflichtet werden, die Daten seiner Gegenstände zur Verfügung zu stellen.[132] Auch könnte anstelle eines öffentlichen Aufrufs an potenzielle Zeugen nach einem Verbrechen die freiwillige Freigabe der persönlichen sensorischen Datenbanken einer ganzen Bevölkerungsgruppe treten, die zusammen mit hoch entwickelten Suchalgorithmen eine Rasterfahndung ungeahnten Ausmaßes erlauben würde. Dabei würden sich all diejenigen verdächtig machen, die sich weigern,

[129] S. kritisch Roßnagel/Pfitzmann/Garstka (Fn. 21), 77f.

[130] S. oben 103 f. (Risiken).

[131] S. z.B. Herrtwich/Rehborn/Franz/Wex 2006, 138 ff.; Roßnagel 2006, 154; s. hierzu auch www.vision-zero.com

[132] S. zu einem Beispiel der Strafverfolgung s. Mattern 2007b, 32f.

den Sicherheitsbehörden den uneingeschränkten Zugriff auf ihre »digitalen Gedächtnisse« einzuräumen.[133] Erweisen sich beispielsweise die Daten aus Fahrzeugsystemen als geeignetes Mittel zur Wahrheitsfindung, könnte der Gesetzgeber fordern, dass die verschiedenen verkehrstelematischen Anwendungen und Dienste die von ihnen verarbeiteten Daten jeweils für die letzten fünf Minuten oder für den letzten gefahrenen Kilometer speichern, damit sie nach einem Verkehrsunfall von der Polizei ausgelesen und für Beweiszwecke gespeichert werden können.[134] Eine ähnliche Zweckänderung könnte auch darin bestehen, die Daten aus Kommunikationsdiensten auszuwerten, um Verkehrsverstöße zu erkennen oder zu beweisen. So könnte einer Übersicht darüber, wo genau sich welches Fahrzeug wann aufgehalten hat, entnommen werden, wer auf welchem Streckenabschnitt zu schnell gefahren ist, verkehrt in einer Einbahnstraße gefahren ist oder ein Rotlicht übersehen hat. Für diese Zweckänderungen wäre eine spezifische gesetzliche Erlaubnisnorm notwendig.[135]

Allgegenwärtige Datenverarbeitung bringt umfangreiche und aussagekräftige personenbezogene Daten hervor, die für Sicherheitsinstitutionen von größtem Interesse sind. Haben viele Dinge jeweils ein »Gedächtnis«, können mit deren Hilfe viele Situationen in der Vergangenheit rekonstruiert werden.[136] Bisher haben die Gesetzgeber früher oder später dem Drängen der Sicherheitsbehörden, auch auf die Daten neuer Anwendungen zugreifen zu können, immer nachgegeben.[137] Einschränkungen gab es allenfalls in der Frage, ob ein Verdacht und eventuell hinsichtlich welcher Straftaten vorauszusetzen ist und ob in irgendeiner Weise ein Richter zu beteiligen ist. Daher muss damit gerechnet werden, dass alle personenbezogenen Daten, die in Alltagsgegenständen verarbeitet werden, über kurz oder lang entgegen ihrem

[133] Mattern 2003c, 34.
[134] S. Roßnagel 2006, 154.
[135] S. Roßnagel 2006, 154.
[136] S. hierzu näher oben 103 f. (Risiken).
[137] S. die Diskussion zum Zugriff der Strafverfolgungsbehörden auf die Daten aus dem Toll-Collect-System – s. hierzu näher Garstka 2006, 129 f.

ursprünglichen Verarbeitungszweck diesen Institutionen zur Verfügung gestellt werden müssen. Ist die Zweckänderung durch Gesetze erlaubt, dürfen die ermächtigten Behörden diese Daten anfordern und für ihre Zwecke verarbeiten.[138] Die Verpflichtung zur Vorratsdatenspeicherung bei Anbietern öffentlicher Kommunikationsdienste ist nur ein Schritt auf diesem Weg.[139] Für all die auf Vorrat gespeicherten Daten könnte die neue Pflicht von Providern, Auskunft über die Nutzer und die Nutzung ihrer Dienste zu geben, um den Berechtigten zu helfen, ihre Urheberrechte durchzusetzen,[140] leicht ausgedehnt werden auf die Durchsetzung von Rechten an Dingen oder auf eine Rechtsverfolgung, für die das Gedächtnis der Dinge ein taugliches Beweismittel sein kann.

3.4.5 Erforderlichkeit und Datensparsamkeit

Das Prinzip der Erforderlichkeit begrenzt den Grundrechtseingriff, der in jeder Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu sehen ist, inhaltlich, modal und zeitlich auf das unbedingt Erforderliche. Es dürfen nur die Daten verarbeitet werden, die für das Erreichen des Zwecks unabdingbar sind. Darüber hinaus gehend fordert das Prinzip der Datensparsamkeit die Datenverarbeitungssysteme so zu gestalten, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden.

Da das Prinzip der Erforderlichkeit am Zweck der Datenverarbeitung ausgerichtet ist, erleidet es hinsichtlich seiner Begrenzungsfunktion 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

[138] S. auch BSI 2004, 47.
[139] S. Roßnagel, EuZ 2006, 30 ff.
[140] S. z.B. den Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten am geistigen Eigentum sowie Art. 8 der zugrunde liegenden EG-Richtlinie 2004/48/EG, s. hierzu auch Raabe, ZUM 2006, 439 ff.

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, also laufend aktualisierenden Weise, begrenzt zudem die Begrenzungsfunktion des Erforderlichkeitsprinzips.[141] Sensorbestückte Gegenstände und Umgebungen sind fast immer aktiv und erheben eine Unmenge Daten, um den Nutzern nach ihrem – sich ständig ändernden – Bedarf jederzeit ihre Dienste anbieten zu können.[142] Hierzu einige Beispiele:

Die Fähigkeit, Objekte zu identifizieren, ermöglicht, die Gegenstände, die den Menschen umgeben, mit einem »Gedächtnis« auszustatten. Die Gegenstände nehmen ihre Umgebung wahr, generieren Daten selbst, tauschen sie untereinander aus und speichern sie auf »ihrer Homepage«.[143] Nutzen die Betroffenen diese Gedächtnisfunktion der Gegenstände, um dadurch ihr eigenes löchriges Gedächtnis zu erweitern, lässt dies das Erforderlichkeitsprinzip gänzlich leer laufen. Für diese Funktion sind alle Daten für sehr lange Zeit erforderlich, weil niemand wissen kann, an was man sich irgendwann einmal erinnern möchte.

Setzt sich die Geschäftsidee des »Pay per Use« durch, die darauf aufbaut, viele Gegenstände nicht mehr zu kaufen, sondern nur noch im Maß des Gebrauchs zu bezahlen,[144] erfordert dies eine Protokollierung der Nutzungen – eventuell auch der Art der Nutzungen – durch die in die Gegenstände integrierten Informationssysteme und die Übertragung der Daten an den Verleiher.[145] Ähnliche Datenverarbeitungen sind erforderlich für die Umsetzung der Geschäftsidee der Autoversicherung, die Prämie dynamisch von dem mehr oder weniger riskanten Umgang mit

141 S. Roßnagel/Müller, CR 2004, 631.
142 S. Roßnagel 2005a, 66; Mattern 2005a, 18.
143 S. oben 43 ff.; s. näher Fleisch/Dierkes 2003, 149; Mattern 2004, 327; Mattern 2005a, 15, 17, 24 ff.; Mattern 2005b, 61 f.
144 S. näher oben 81.
145 S. z.B. auch Mattern 2005a, 22.

dem Fahrzeug abhängig zu machen.[146] Das Gleiche gilt, wenn die Kunden im Einzelhandel damit einverstanden sind, dass je nach Einkaufsverhalten eine personenbezogene Preisdifferenzierung stattfindet.[147]

Aus vergleichbaren Zwängen stößt auch der Grundsatz, möglichst keine oder wenige personenbezogene Daten zu erheben, zu speichern und zu verarbeiten, an Grenzen. Oft kann erst eine Vielzahl langfristig gespeicherter Daten die Unterstützungsleistung bieten, die mit der Nutzung von Ubiquitous Computing erreicht werden soll.

Zum einen gerät die Datensparsamkeit in Widerspruch zu vielen gewünschten Anwendungen: Die meisten Träume, die mit allgegenwärtiger Datenverarbeitung verbunden werden, lassen sich nur verwirklichen, wenn das Prinzip der Datensparsamkeit ignoriert wird. Systeme, die die »Gedächtnisleistung« der Menschen verbessern sollen, müssen so gestaltet sein, dass sie sich an möglichst viele Ereignisse erinnern können. Systeme, die kontextbezogen die Menschen von Arbeit entlasten sollen, werden viele Daten benötigen, deren Relevanz auf den ersten Blick nicht gegeben ist, die aber in Kombination oder im Vergleich mit anderen Daten den Kontext und damit das Ziel und die Art und Weise der Entlastung erschließen. Sie müssen für ihre Funktionserfüllung auch viele Daten »auf Verdacht« erheben und verarbeiten.[148] Ähnlich verhält es sich mit der Funktion der Sicherheitsgewährleistung. Um keine Lücken in dem »Sicherheitsgürtel« um ein Gebäude oder ein Gebiet entstehen zu lassen, sind alle Daten zu verarbeiten, die durch die Rundum-Beobachtung entstehen oder die durch Sensornetze erhoben werden. Wenn solche Daten – insbesondere in Sensornetzen – ohnehin entstehen, würde es dem Prinzip der Vorsorge widersprechen, sie mutwillig zu ignorieren oder zu löschen. Sie könnten Hinweise auf Unregelmäßigkeiten enthalten, die sicherheitsrelevant sein können.

146 S. oben 83 f.
147 S. oben 74 ff.
148 Langheinrich 2005a, 340.

Zum anderen könnten Mechanismen der Datensparsamkeit, nämlich die Verwendung anonymer oder pseudonymer Daten durch Techniken allgegenwärtiger Datenverarbeitung an Bedeutung verlieren. Selbst wenn anonyme und pseudonyme Daten verarbeitet werden, kann dies für den Zweck, den Personenbezug zu vermeiden, ungeeignet sein. So kann beispielsweise der Personenbezug trotz Anonymität hergestellt werden, wenn für die allgegenwärtige Datenverarbeitung die Daten unmittelbar erhoben werden: Eine Kamera, ein Mikrofon, ein Sensor oder ein Indoor-Lokalisierungssystem nehmen anders als ein Webformular den Benutzer direkt wahr und können vielfach[149] 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 bei allgegenwärtiger Datenverarbeitung typische enge Verknüpfung der Sensorinformation mit Ereignissen der realen Welt erlaubt selbst bei konsequenter Verwendung von anonymen oder pseudonymen Daten in vielen Fällen eine einfache Personenidentifikation – etwa bei einem Indoor-Lokalisierungssystem anhand des bevorzugten Aufenthaltsorts einer Person.[150]

Auch kann die Wahrscheinlichkeit, anonymisierte oder pseudonymisierte Daten zu deanonymisieren, durch allgegenwärtige Datenverarbeitung erheblich ansteigen. Mit ihr nimmt die zeitliche und räumliche Dichte der von Personen hinterlassenen Datenspuren erheblich zu. Dies verbessert aus rein statistischen Gründen die Möglichkeit, zu diesen den Personenbezug herzustellen.[151] Dies gilt auch für potenziell personenbezogene Daten, zu denen etwa die Kennziffern von RFID-Tags oder Sensordaten

[149] Für Kameras könnte die Technik des Privacy-Filters, der Gesichter »verwürfelt« und nur nach zusätzlicher Freigabe kenntlich macht, Anwendung finden – s. z.B. Stechow 2005.

[150] S. Langheinrich 2005a, 339f.; Fabian, in: TAUCIS 2006, 249.

[151] S. hierzu BSI 2004, 47.

gehören. Die Vielfalt solcher Daten erhöht die Wahrscheinlichkeit, dass rückwirkend plausible Schlüsse auf Einzelpersonen gezogen werden können.

3.4.6 Betroffenenrechte

Sollen die Betroffenen nicht nur Objekte der Datenverwendung und -nutzung sein, benötigen sie Mitwirkungsrechte, die ihnen Einfluss darauf ermöglichen, ob und wie die auf sie bezogenen Daten verarbeitet werden. Diese Rechte der Betroffenen werden aber 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 Betroffenen es erheblich erschweren, diese Rechte geltend zu machen.[152] Bei dem Versuch, dies zu tun, werden die beschriebenen Einschränkungen, Zersplitterungen und Intransparenzen der Verantwortlichkeit[153] praktisch wirksam werden. 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.[154]

Hinsichtlich der Organisation der Datenverarbeitung gibt es allein schon datenschutzrechtlich unterschiedliche Zielsetzungen. So wird zum Beispiel die Erfassung und Überwachung des Betroffenen erschwert, wenn die Daten dezentral und spontan verarbeitet werden. Eine solche Organisation der Datenverarbeitung erschwert aber zugleich die Wahrnehmung von Betroffenenrechten. Der Einzelne sieht sich einer Unzahl von Akteuren,

[152] S. Roßnagel/Pfitzmann/Garstka 2001, 22 ff., 185f.; Roßnagel/Müller, CR 2004, 631; Mattern 2005a, 26f.; Möller/Bizer, in: TAUCIS 2006, 119.

[153] S. oben 128ff.

[154] S. Roßnagel 2005a, 66.

einer Zersplitterung der Verarbeitungsvorgänge und einer Diffusion von Verantwortlichkeit für die Verarbeitung seiner personenbezogenen Daten gegenüber.

Ein weiteres Problem für die Wahrnehmung von Betroffenenrechten ist die Unmerklichkeit der Datenerhebung. Allgegenwärtige Datenverarbeitung lässt sie unsichtbar werden. Erhebung und Verarbeitung von Daten sind in die Umgebung integriert und werden damit zum normalen Bestandteil von Handlungen und Verhalten. Soll die Interaktion mit Rechnertechnik so weit in den Hintergrund treten, dass man sie gar nicht mehr bemerkt, tritt aber auch eine damit verbundene Datensammlung in den Hintergrund. Allgegenwärtige Datenverarbeitung kann den Nutzer von aktiver Teilnahme so weit entlasten, dass sie letztlich unmöglich wird.

Zudem werden die Datenverarbeitung und ihr Ergebnis nicht von einem Sensor oder einem RFID-Tag allein bewirkt, sondern durch das Zusammenarbeiten einer Vielzahl von Datenverarbeitungen im Hintergrund. Der Betroffene nimmt die einzelne Datenerhebung in der Regel nicht wahr und, wenn er dies dennoch tut, kann er die gesamte Datenverarbeitung nur schwer nachvollziehen. Betroffenenrechte geltend zu machen, wird somit auch durch diese Eigenschaften allgegenwärtiger Datenverarbeitung sehr erschwert.[155]

Will er etwa Auskunft über die Daten, die ein Sensor oder ein Sensornetz über ihn aufgenommen hat, wird ihm statt eines einfachen Datensatzes wie etwa die Postadresse ein komplexes Destillat aus ihm unverständlichen Daten präsentiert werden müssen. Dieses erlaubt in den meisten Fällen nur eine Vermutung, nicht aber die Feststellung, dass es den Betroffenen betrifft.[156] Ähnliches gilt für die Auskunft über den Inhalt eines RFID-Chips.[157] Will er wissen, wer die Sensordaten oder die RFID-

[155] S. ebenso Möller/Bizer, in: TAUCIS 2006, 204.

[156] S. auch Langheinrich 2005, 340; Mattern 2007b, 31.

[157] S. Artikel-29-Datenschutzgruppe 2005a, 16.

Kennung erhoben und verarbeitet hat, wird er diese Stellen nur ausfindig machen können, wenn sie in einem einfach strukturierten Verhältnis zwischen verantwortlicher Stelle und Betroffenen verarbeitet werden.[158] In einem offenen System, in dem »jeder« oder »viele« die Sensordaten oder die RFID-Kennung »abgreifen« können, wird er die potenziellen Stellen, von denen er Auskunft verlangen müsste, nicht ermitteln können – zumindest solange die »abgreifenden« Stellen sich nicht identifizieren müssen und die Sensoren oder RFID-Tags dies nicht protokollieren.[159]

Automatisierte Entscheidungen, die auf der Bewertung einzelner Persönlichkeitsmerkmale basieren und für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich belasten, sind nach § 6a BDSG unzulässig. Würde dieser Schutz des Betroffenen so verstanden, dass als automatisierte Entscheidung gilt, wenn der Betroffene zum Beispiel in einem Ladengeschäft automatisch erkannt und begrüßt oder abgewiesen wird, wenn er in einem Zimmer automatisch erkannt, seine Bedürfnisse bezüglich Klima und Raumtemperatur identifiziert und die Umgebungsbedingungen entsprechend seinen Präferenzen reguliert werden oder dass in einem Kraftfahrzeug die Komforteinstellungen wie Sitzhöhe und Rückspiegel spezifisch für ihn automatisch erfolgen,[160] dann würden alle Entlastungen von Arbeit, alle Maßnahmen zur Erhöhung des Komforts und alle Aktionen zur Erhöhung der Sicherheit verboten sein, wenn sie nicht den Erwartungen des Betroffenen entsprechen. Ein solches Verständnis des Betroffenenschutzes würde in einer Welt allgegenwärtiger Datenverarbeitung, die ja gerade Arbeitsentlastung, Komfortsteigerung und Sicherheitsgewährleistung durch Delegation von Aufgaben auf Technik erreichen will, als praxisuntauglich verstanden.[161]

[158] S. hierzu oben 120 ff.

[159] S. zur technischen Möglichkeit unten 160.

[160] So die Beispiele in Möller/Bizer, in: TAUCIS 2006, 217.

[161] Bereits nach geltendem Recht unzutreffend ist das Beispiel des selbstständig nachbestellenden Kühlschranks, der für seinen Besitzer selbständig Vertragsverhältnisse mit Lebensmittellieferanten abschließt und ihn zur Abnahme sowie zur Zahlung verpflichtet – so Möller/Bizer, in: TAUCIS 2006, 217. Hier wird vom Betroffenen ein

Schließlich versagen die datenschutzrechtlichen Betroffenenrechte, wenn die Datenerhebung und -verarbeitung – etwa durch Wearable Computing – ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.[162] Wenn Sensoren, Minikameras, Lokalisatoren und Prozessoren in Kleidungsstücke integriert sind, wird potenziell jeder zum ständigen Datensammler.[163] Er ist zugleich Betroffener der Welterfassung durch andere Nutzer allgegenwärtiger Datenverarbeitung und selbst Datenverarbeiter durch seine Wearable Computing-Anwendungen. Da seine Datenerhebung, -verarbeitung und -nutzung aber außerhalb des Datenschutzrechts stattfindet, haben die davon Betroffenen keine Datenschutzrechte. Sie können allenfalls – ohne Unterstützung durch Kontrollstellen – unter engen Voraussetzungen Ansprüche auf Unterlassung oder Löschung nach §§ 823, 1004 BGB gerichtlich geltend machen.[164]

3.4.7 Kontrolle

Die Durchsetzung des Rechts auf informationelle Selbstbestimmung erfordert unabhängige externe Kontrollstellen, die auf Hinweise der Betroffenen oder anlassunabhängig die Datenverarbeitungspraxis überprüfen. Um innerhalb der verantwortlichen Stellen die Verantwortung für die Einhaltung datenschutzrechtlicher Vorgaben sicherzustellen und dem Datenschutz einen angemessenen Platz in der Kommunikation und Willensbildung zu sichern, wirken in mittleren und großen verantwortlichen Stellen betriebliche oder behördliche Datenschutzbeauftragte.[165]

Softwareagent benutzt, dessen »Willenserklärungen« dem Betroffenen zuzurechnen sind – s. hierzu Roßnagel/Gitter, K&R 2003, 63 ff.; Gitter, in: Gitter/Lotz/Pinsdorf/Roßnagel 2007, 46 ff.; Gitter 2007, 155 ff.; Cornelius, MMR 2002, 353 ff. Dies gilt für alle Beispiele, bei denen die Nutzung automatisierter Entscheidungsverfahren vom Betroffenen eingesetzt wird.

162 S. hierzu oben 131 ff.

163 S. hierzu oben 70 f.

164 S. näher oben 120 ff.

165 S. oben 118.

Die Aufsichtsbehörden haben zwar mittlerweile die Möglichkeit, auch ohne einen konkreten Anlass die Datenverarbeitung einer verantwortlichen Stelle zu prüfen, die Ressourcen sind aber so beschränkt, dass bereits heute mit regelmäßigen und flächendeckenden Kontrollen nicht zu rechnen ist.[166]

Diese unbefriedigende Situation wird sich künftig allein durch die enorme Zunahme an personenbezogenen Daten dramatisch verschlechtern. Hinzu kommt die Charakteristik neuer Anwendungen, die durch ihre Dynamik, ihre Vielfalt und Komplexität gekennzeichnet ist. Vielfach werden diese Anwendungen nicht langfristig entwickelt und eingeführt, sondern spontan entstehen und wieder vergehen, bevor eine Kontrollstelle überhaupt gemerkt hat, dass diese Anwendung existiert und personenbezogene Daten verarbeitet. All dies wird dazu beitragen, dass die Verwendung personenbezogener Daten im Rahmen allgegenwärtiger Datenverarbeitung die Kontrollkapazität der Aufsichtsbehörden um ein Vielfaches übersteigt.[167] Allein bereits die personelle Ausstattung der Aufsichtsbehörden wird es verhindern, dass sie der informationellen Selbstbestimmung gesellschaftlich wirklich zur Durchsetzung verhelfen können.

Die Datenschutzaufsicht wird sich allenfalls auf stichprobenartige und anlassbezogene Überprüfungen einzelner großer Datenverarbeiter konzentrieren können. In solchen Einzelprüfungen kann sie sich die Systeme allgegenwärtiger Datenverarbeitung ansehen und erklären lassen. Mangelnde Transparenz, unzulässige Datenverarbeitung ohne Einwilligung und Zweckänderungen, die nicht von Erlaubnistatbeständen gedeckt sind, können dabei auffallen und angemahnt werden. Für diese Datenverarbeiter wird auch ein betrieblicher Datenschutzbeauftragter ernannt sein, der sich auch bei Planung und Einsatz allgegenwärtiger Datenverarbeitung betriebsintern für die Einhaltung des Datenschutzrechts einsetzen kann. Bei großen, von Unternehmen oder

166 S. Möller/Bizer, in: TAUCIS 2006, 218.

167 S. im Ergebnis ebenso Möller/Bizer, in: TAUCIS 2006, 204.

Behörden geplanten Anwendungen allgegenwärtiger Datenverarbeitung kann auch das Instrument der Vorabkontrolle nach § 4d Abs. 5 und 6 BDSG zum Einsatz kommen.[168]

Die große Zahl der kleinen Unternehmen muss jedoch keinen Datenschutzbeauftragten bestellen[169] und keine Vorabkontrolle durchführen.[170] Aber auch die noch um ein Vielfaches größere Anzahl der einzelnen Personen, die jeweils viele Anwendungen allgegenwärtiger Datenverarbeitung für sich oder im gesellschaftlichen Kontakt mit anderen nutzen, wird von diesen Kontrollinstrumenten nicht erfasst.[171] Soweit sie überhaupt der Kontrolle durch die Aufsichtsbehörden unterstehen, gelten für diese die bereits beschriebenen Einschränkungen, Zersplitterungen und Intransparenzen der Verantwortlichkeit.[172] Sie führen dazu, dass die Handlungsmöglichkeiten der Aufsicht in vergleichbarer Weise eingeschränkt sind wie diejenigen der Betroffenen.[173]

Viele Anwendungen allgegenwärtiger Datenverarbeitung werden schon deswegen aus der Datenschutzkontrolle herausfallen, weil sie ausschließlich für persönliche und familiäre Zwecke genutzt

168 S. zu einfach strukturierten Verhältnissen auch oben 120 ff.

169 Nach § 4f Abs. 1 BDSG erst ab 20 Mitarbeiter, die mit personenbezogener Datenverarbeitung befasst sind.

170 Nach § 4d Abs. 5 BDSG ist die Vorabkontrolle durchzuführen, soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Beruhigungen, wie die von Möller/Bizer, in: TAUCIS 2006, 204, für jede der vielfältigen Anwendungen kleiner Unternehmen sei aufgrund ihrer systemimmanenten Komplexität und des damit gesteigerten Risikos für das informationelle Selbstbestimmungsrecht eine Vorabkontrolle durchzuführen und deshalb hätten diese einen betrieblichen Datenschutzbeauftragten unabhängig von der Anzahl der mit personenbezogener Datenverarbeitung befassten Mitarbeiter zu bestellen, der fachlich qualifiziert ist, eine solche Vorabkontrolle durchzuführen, erscheinen lebensfremd: Erwartungen, es würden für viele Millionen Anwendungen Vorabkontrollen durchgeführt und kleine Unternehmen mit ein, zwei oder drei Mitarbeitern könnten einen Datenschutzbeauftragten beschäftigen, sind illusorisch.

171 Daher werden die Erwartungen, die Möller/Bizer, in: TAUCIS 2006, 224, in diese Kontrollinstrumente haben, vielfach enttäuscht werden.

172 S. oben 128 ff.

173 S. oben 149 ff.

werden.[174] Dies wird vor allem für die Anwendungen im eigenen Haus oder in der eigenen Wohnung, in deren unmittelbarem Umkreis, im eigenen Kraftfahrzeug oder bei Anwendungen rund um die eigene Person der Fall sein. Dabei handelt es sich keineswegs immer um kleine, kurz greifende, selten genutzte und daher vernachlässigbare Anwendungen. Vielmehr können diese sehr mächtig, ständig genutzt, breit wirksam und tief in die informationelle Selbstbestimmung eingreifend sein.

Wirksam – allerdings nur für Extremfälle – könnte durch seine Abschreckungswirkung ein strafrechtlicher Schutz werden. Dieser besteht momentan, wenn jemand im Rahmen der Kommunikation von Gegenständen untereinander oder mit ihren Nutzern personenbezogene Daten rechtswidrig zur Kenntnis nimmt oder wenn er Daten verändert oder unterdrückt.[175] Fraglich ist jedoch, ob und inwieweit angesichts der geschilderten Probleme bei der Nachvollziehbarkeit von Handlungen und der Verflüchtigung von Verantwortlichkeit Täter ermittelt und eine Tat nachgewiesen werden können.[176]

3.5 Die Zukunft des normativen Schutzprogramms

Fasst man alle diese Entwicklungen und ihre Auswirkungen zusammen, muss man feststellen: Alle Bestandteile des überkommenen Schutzprogramms werden durch Ubiquitous Computing ausgehöhlt oder überspielt. Wird sich das Recht dagegen wehren und seine Beachtung einfordern können? Wird das Datenschutzrecht diese Entwicklung »bremsen« können?[177]

Für die Beantwortung der Frage ist zu beachten, dass es sich hier nicht um ein Vollzugs-, sondern um ein Konzeptproblem handelt. Es geht nicht nur darum, den Prinzipien des Daten-

174 S. hierzu oben 131 ff.

175 Müller, DuD 2004, 215 ff.; Holznagel/Bonnekoh 2006, 46 ff., 54 ff.

176 S. auch Möller/Bizer, in: TAUCIS 2006, 212.

177 So Möller/Bizer, in: TAUCIS 2006, 216.

schutzes in einer ihnen ungünstigen Welt durch entschlossenes Handeln Geltung zu verschaffen. Vielmehr sind die Prinzipien des Datenschutzes – jedenfalls in ihrer Ausprägung durch das geltende Datenschutzrecht – und die Prinzipien allgegenwärtiger Datenverarbeitung nicht zu vereinbaren. In einem Konflikt zwischen beiden ist jedoch nicht zu erwarten, dass sich das Datenschutzrecht in breiter Front durchsetzen wird.

Nur hinsichtlich weniger Ausnahmen wird die Nutzung allgegenwärtiger Datenverarbeitung verordnet und durchgesetzt werden können. Dies gilt für staatlich kontrollierte Systeme, deren Nutzung etwa im Straßenverkehr zur Mauterhebung oder zur Durchsetzung von Verkehrsregeln erzwungen wird. Auch ist zu erwarten, dass wirtschaftliche Macht dazu genutzt wird, die Nutzung von Ubiquitous Computing-Anwendungen durchzusetzen. Dies könnte zum Beispiel der Fall sein, wenn Waren mit RFID-Tags eingeführt werden, ohne den Kunden Wahlmöglichkeiten zu lassen. In diesen Fällen könnte es sein, dass sich viele Betroffene auf ihre Datenschutzrechte berufen. Eventuell könnte dann breiter Widerstand ermöglichen, datenschutzrechtliche Prinzipien zumindest in den dann zu findenden Kompromissen zur Geltung zu bringen. Dies betrifft jeweils einfach strukturierte Verhältnisse, in denen es auch künftig möglich sein wird, Datenschutz in der bisherigen Weise zur Geltung zu bringen.[178]

Dagegen wird die neue Welt allgegenwärtiger Datenverarbeitung in dem hier beschriebenen Umfang nur dann Wirklichkeit werden, wenn sie in ihren wichtigsten Anwendungen individuell, gesellschaftlich und politisch gewollt wird. Dies wird bei den meisten Anwendungen der Fall sein. Sie 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 und sicherer machen. Sie werden individualisierte Dienste und Geräte fordern, die sich ihnen anpassen,

[178] S. hierzu oben 120 ff.

sie bei ihren Tätigkeiten scheinbar mitdenkend begleiten und ihnen in einer sich selbst organisierenden Weise kontextbezogen die jeweils benötigte Unterstützung bieten. Sie werden dann als Konsequenz auch damit einverstanden sein müssen, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweise, Gewohnheiten, Einstellungen und Präferenzen erhalten. Wenn sie ihr Haus, ihr Auto und sich selbst technisch aufrüsten und mit ihrer allgegenwärtigen Informationstechnik die Daten anderer Menschen erheben und verarbeiten, können sie schlecht verlangen, dass andere dies bezogen auf sie unterlassen.

Wenn breit akzeptiert ist, dass die Technik den Nutzer unmerklich unterstützen soll, haben die geltenden Transparenzanforderungen wenig Chancen. Wenn die Technik eingesetzt wird, um das Gedächtnis zu unterstützen, sind die Begrenzung auf einen Zweck oder eine frühzeitige Löschung kontraproduktiv. Wenn Dienste nach Bedarf kreiert und genutzt werden sollen, empfindet jeder eine vorherige Vorabuntersuchung als schikanös. Wenn allgegenwärtige Datenverarbeitung gewollt ist, wird es kaum möglich sein, Datenschutz in seiner bisherigen Ausprägung gegen die konträren Grundideen dieser Technikanwendung zu realisieren.[179]

[179] S. hierzu näher Roßnagel/Müller, CR 2004, 617 ff.; Roßnagel, NVZ 2006, 288.

4. DATENSCHUTZTECHNIK

Soweit normativer Datenschutz an konzeptionelle Grenzen stößt oder Probleme in der Durchsetzung hat, besteht die Hoffnung, dass die Datenschutzziele durch Technik erfüllt werden können. Zur Durchsetzung oder Unterstützung von Datenschutz müssten adäquate technische Mittel zur Verfügung stehen. Ohne diese bleibt ein effektiver Datenschutz illusorisch, mit diesen wäre aber langfristig vielleicht sogar eine nachhaltige Verbesserung heutiger Bedingungen denkbar.[1]

Sind geeignete technische Instrumente nicht verfügbar, ist daran zu arbeiten sie zu entwickeln. Ohne sie gerät die Informationsgesellschaft in ein Entwicklungsdilemma. Je mehr Techniken allgegenwärtiger Datenverarbeitung zur Freiheitsförderung zum Einsatz kommen, desto mehr personenbezogene Daten werden verarbeitet und desto mehr wachsen ihre freiheitsbedrohenden Kontrollpotenziale. Je mehr Lebensbereiche unterstützt werden, desto mehr Lebensäußerungen werden durch die Auswertung von personenbezogenen Daten erfasst. Jede personalisierende Informationstechnikanwendung erhöht zugleich das Überwachungspotenzial. Eine allgegenwärtige Unterstützung erfordert eine so umfassende Verarbeitung von Daten, dass aus diesen nahezu das gesamte Leben rekonstruiert werden könnte. Das Dilemma erscheint unausweichlich: Jede gewünschte und sinnvolle personalisierte Nutzung von Informationstechnik führt zwangsläufig zu mehr Überwachung.[2]

Dieses Dilemma ist nur zu vermeiden, wenn Techniken entwickelt werden, die ermöglichen die Verbindung zwischen technischer Dienstleistung und Personalisierung aufzubrechen und die gewünschten Dienstleistungen auch ohne personenbezogene Daten anzubieten. Soweit dies nicht möglich ist, müssen die Betroffenen technisch unterstützt werden, ihre informationelle Selbstbestimmung so weit wie möglich zu wahren. Hierfür könnte die Metapher eines »Datenschutzagenten« hilfreich sein, einer software-technischen Unterstützung, die dem Betroffenen Datenschutzarbeit abnimmt und ihm hilft, Datenverwendungen zu erkennen und auf sie zu reagieren. Auch für den Datenschutz darf der Traum gelten, dass eine Delegation auf Technik vom Zwang zur Aufmerksamkeit befreit, von Arbeit entlastet und die Wirksamkeit des Handelns erhöht.

Im Folgenden werden einige Techniken beschrieben, die helfen, Datenschutzanforderungen durchzusetzen. Sie sind allerdings bisher kaum über Konzeptionen und Demonstrationen hinaus gekommen. Die meisten betreffen den Datenschutz in RFID-Anwendungen.

4.1 Transparenz

Die Datenschutztransparenz leidet in einer Welt allgegenwärtiger Datenverarbeitung unter anderem an subjektiven Überforderungen.[3] Statt den Betroffenen hinsichtlich möglicher Datenerhebungen und -verarbeitungen in Dauerstress zu versetzen, ist es notwendig, dass ein technisches System automatisch diese erkennt, die verantwortliche Stelle identifiziert und die Relevanz der Datenverwendung einschätzt. Nur in schwierigen Einzelfällen oder auf Wunsch des Betroffenen wird dieser involviert. Das Ziel muss sein, eine Überbeanspruchung der Nutzer durch eine »Transparency on Demand« so weit wie möglich zu vermeiden.[4]

[1] Langheinrich 2005, 338; Müller/Handy, DuD 2004, 659.
[2] S. hierzu für die Personalisierung Roßnagel, WI 2007, 14.
[3] S. oben 133 f.
[4] Ähnlich auch Langheinrich 2005a, 338.

4.1.1 Automatische Erkennung der Datenerhebung

Ein einfacher Ansatz zum Schutz vor unbemerktem Auslesen wäre ein Gerät, das die Aktivität von Sensoren, Kameras, Mikrophonen oder Lesegeräten erkennt und diese dem Nutzer anzeigt.[5] Zusätzlich könnte ein solcher Datenerhebungs-Warner mit einer Protokollierungsfunktion ausgestattet werden, mit der sämtliche Erhebungs-, Lese- und Schreibvorgänge sowie deren Versuche aufgezeichnet werden können. Zugriffe könnten auch auf dem RFID-Chip protokolliert werden. Vorstellbar wäre ein Zugriffszähler, der wie bei Webseiten, die Zahl der Zugriffe mitzählt.[6]

Eine aktive Maßnahme der verantwortlichen Stelle wäre es, Mechanismen zur expliziten Ankündigung von Datenerhebungen zu nutzen. Eine solche drahtlos empfangbare, maschinenlesbare Ankündigung könnte über die Mitteilung der beabsichtigten Datenerhebung hinaus weitere Informationen enthalten oder auf solche – zum Beispiel zur Struktur und zur Arbeitsweise der Datenverarbeitung auf der Homepage des kommunikationsfähigen Gegenstands – hinweisen.[7]

4.1.2 Automatische Identifizierung der verantwortlichen Stelle

Sinnvoll einsetzbar wäre der Warner allerdings nur, wenn auch jedes Lesegerät eindeutig identifizierbar ist. Hierfür könnte eine eindeutige Reader Policy ID (RPID) eingeführt werden, die beim Auslesen der RFID-Tags vom Lesegerät automatisch mitgesendet wird.[8] Die damit verbundenen Informationen über den Betreiber des Lesegeräts könnten mit Hilfe des Warngeräts für den Betroffenen sichtbar gemacht oder akustisch mitgeteilt werden. Damit würde ihm – bei Bedarf und Interesse – zu einem gewissen Grad

[5] Bartels/Ahlers, c't 9/2004, 132 ff.
[6] S. hierzu Müller/Handy, DuD 2004, 657.
[7] Langheinrich 2005a, 338.
[8] S. Flörkemeier/Schneider/Langheinrich 2004; Müller/Handy, DuD 2004, 657; BSI 2004, 54.

die Möglichkeit gegeben, die Funktion der Tags zu kontrollieren und die Verwendung der ausgelesenen Daten zu verstehen. Bei Verletzung von Datenschutzanforderungen könnte der Betreiber des Lesegeräts identifiziert und zur Verantwortung gezogen werden.[9]

4.1.3 Datenschutzkommunikation

Erkennen der Erhebung und Identifizierung der verantwortlichen Stelle könnte zu einem automatisierten Austausch über die jeweils geltende Datenschutzpolitik fortentwickelt werden. Ein solches Protokoll besteht in der Form der »Platform for Privacy Preferences (P3P)«[10] bereits für das WWW und könnte auch in modifizierter Form für Anwendungen allgegenwärtiger Datenverarbeitung eingeführt werden. Eine solches »Privacy Awareness System« wurde bereits konzipiert.[11] Im Kern steht die Definition von Datenschutz-Präferenzen durch den Nutzer für den Umgang mit seinen personenbezogenen Daten. Diese Präferenzen werden automatisch mit den digital hinterlegten Datenschutzregeln von Diensten abgeglichen. Stimmen Präferenzen und Regeln überein, wird die Erhebung erlaubt oder werden die personenbezogenen Daten übergeben. Widersprechen sich beide, wird die Datenerhebung oder -übergabe unterbunden oder der Betroffene gewarnt. Die Hinweis- und Warndichte muss einstellbar sein.

4.2 Selbstbestimmung

Die Ausübung von Selbstbestimmung findet vor allem in Form von Einwilligungen in die Datenerhebung oder -verarbeitung statt. Angesichts der übermäßigen Fülle der Erhebungsvorgänge

[9] Zu einer zusätzlichen Authentifizierung s. z.B. Fabian, in: TAUCIS 2006, 270 ff.
[10] Platform for Privacy Preferences – s. näher www.w3c.org/P3P.
[11] Langheinrich 2005b, 115 ff.; ähnlich Yamada/Kamioka, IEICE Transactions on Communication 3/2005, 853f.; s. auch BSI 2006, 94; Fabian, in: TAUCIS 2006, 282 ff., 304 ff.

kann aber auch die Wahrnehmung eines Grundrechts zu Überbeanspruchungen führen. Statt im Sekundentakt vom Betroffenen eine Entscheidung zu verlangen, sollte ein automatisches System einen Großteil der Entscheidungen selbst treffen und allenfalls vereinzelt nachfragen.[12]

4.2.1 Einwilligungsunterstützung

Ein »Privacy Awareness System« kann nicht nur die Transparenz erhöhen, sondern auch dazu genutzt werden, bei einer Übereinstimmung von Präferenzen und Datenschutzpolitik eine automatisch generierte Zustimmung zur Datenverwendung zu erteilen.[13] Diese entspricht zwar nicht den formalen Anforderungen an eine datenschutzrechtliche Einwilligung. Sie könnte aber signalisieren, dass der Betroffene einverstanden ist. Auch könnte an die gesetzliche Einführung einer Form gedacht werden, die den Bedingungen allgegenwärtiger Datenverarbeitung entspricht.

Hinsichtlich der Eindeutigkeit und Belastbarkeit von Datenschutzpräferenzen wurden Zweifel geltend gemacht.[14] Hieran dürfte richtig sein, dass der Abgleich zwischen Datenschutzerklärung und Präferenzen nicht sehr differenziert erfolgen kann. Ob allerdings die schriftliche Einwilligung in die Datenverarbeitung heute von den Betroffenen differenzierter erfolgt, darf ebenfalls bezweifelt werden. Die automatisierte Einwilligung sollte als ein Instrument angesehen werden, das jedem zur Verfügung steht, der es nutzen möchte. Die Auswahl von Präferenzen kann vereinfacht werden, wenn der Betroffene die Datenschutzpräferenzen einer für ihn vertrauenswürdigen Institution übernimmt.

[12] S. z.B. Langheinrich 2005a, 338; Langheinrich 2001, 273 ff; zu recht weist Hubig 2007, 161, darauf hin, dass die daraus erkennbaren Präferenzen ihrerseits wiederum die Preisgabe personenbezogener Daten darstellt.

[13] Langheinrich 2005b, 122 ff.; Langheinrich 2005a, 338.

[14] S. z.B. Langheinrich 2005a, 338.

4.2.2 Entscheidung über die Techniknutzung

Will der Betroffene von der Datenverarbeitung durch datenerhebende und kommunikationsfähige Gegenstände und Umgebungen verschont bleiben, kann er versuchen, zumindest im eigenen Umfeld Sensoren, RFID-Chips und andere Erhebungstechniken zu entfernen. Vielfach genügt es, die Antenne für die Kommunikation zu beseitigen.[15]

Gelingt dies nicht, weil diese zum Beispiel untrennbar mit den Gegenständen verbunden sind, kann er zumindest bei RFID-Chips den »Kill-Befehl« nutzen. Bei diesem wird der RFID-Chip durch einen speziellen Befehl des Lesegerätes komplett und unwiederbringlich deaktiviert.[16] Diese »Kill«-Funktion ist auch in den Standards von EPCglobal vorgesehen. Sie soll ermöglichen, den Chip auf Wunsch eines Kunden beim Verkauf dauerhaft zu deaktivieren. Um einen Missbrauch dieses Befehls zu verhindern, erfordert dieser die Eingabe eines für diesen Chip passenden Passworts.

Dieses Verfahren erscheint allerdings sehr schwierig, wenn man bedenkt, dass Passwörter für Milliarden von Produkten entlang einer ganzen Lieferkette (Zulieferer, Hersteller, Großhändler, Einzelhändler) und über beliebige Verkaufsorte hinweg (Großmarkt, Supermarkt, Detailhändler, Kiosk und Würstchengrill) verwaltet werden müssen.[17] Außerdem werden durch die Deaktivierung auch alle sinnvollen Nutzungen im privaten und geschäftlichen Bereich unterbunden.[18]

[15] S. Fabian, in: TAUCIS 2006, 267f.; Voort/Ligtvoet 2006, 20f.; AK Technik 2006, 15: »Clipped Tags«.

[16] Müller/Handy, DuD 2004, 568; Langheinrich 2006, 13; Langheinrich 2007a, 134; Artikel-29-Datenschutzgruppe 2005a, 17; BSI 2004, 53f.; Holznagel/Bonnekoh 2006, 43; Holznagel/Bonnekoh, MMR 2006, 23; Fabian, in: TAUCIS 2006, 263, 268; Voort/Ligtvoet 2006, 21.

[17] S. z.B. Langheinrich 2007a, 135: »utopisch«.

[18] S. z.B. Langheinrich 2005a, 355; Langheinrich 2007a, 135; Müller/Handy, DuD 2004, 658; Fabian, in: TAUCIS 2006, 267 – s. zur Sekundärnutzung oben 66f. (Logistik).

4.2.3 Datenschutzsphären

Ein anderer Ansatz wird durch die Metapher der »Digital Bubble« beschrieben. Nach diesem Konzept sollen kontextbezogene Filter mehrere, unterschiedlich nahe digitale Räume um den Nutzer herum dadurch schützen, dass sie die Interaktion mit anderen datenverarbeitenden Akteuren kontrollieren. Der Filter kann dabei von ungehindertem Austausch bis zur totalen Blockade reichen. Hierfür werden Profile und Regeln definiert, die den Wünschen des Nutzers entsprechen und zudem Anonymität und Pseudonymität zulassen. Eine Möglichkeit wäre zum Beispiel Sphären um den Nutzer zu definieren, die sich an der Nähe der Datenhaltung zum Nutzer orientieren. Danach könnte etwa der körperliche Bereich alle datenverarbeitenden Gegenstände am oder sogar im Körper betreffen wie Implantate, Brillen und Hörgeräte. Zum privaten Bereich könnten Gegenstände im persönlichen Gewahrsam wie Mobiltelefon oder ein mit RFID-Chip ausgestattetes Kleidungsstück zählen. Die nächsten Schutzkreise könnten durch die familiäre und die berufliche Umgebung gebildet werden.[19]

4.3 Zweckmarkierung

Werden Mechanismen zur expliziten Ankündigung von Datenerhebungen genutzt, könnten diese auch den Zweck, zu dem Daten erhoben werden, mitteilen.[20] Auch wenn dadurch die Zweckbindung noch nicht sichergestellt wäre, sondern der Zweck nur kommuniziert wird, würde eine maschinenlesbare Deklaration es Kontrollstellen und Betroffenen erheblich erleichtern, die Erhebung und eventuell auch die spätere Verwendung zu kontrollieren.[21]

[19] S. z.B. Crutzen 2005; BSI 2006, 93f.

[20] S. z.B. Langheinrich 2005a, 338.

[21] Langheinrich 2007a, 139.

Für das RFID-Umfeld sind Möglichkeiten, den Zweck mitzuteilen und bei der Datenverarbeitung zu berücksichtigen, bereits konzipiert worden. Sowohl Lesegeräte als auch RFID-Chips könnten so programmiert werden, dass sie Daten nur lesen oder freigeben, wenn der richtige Zweck deklariert wird. Damit das Lesegerät erkennen kann, für welche Anwendung ein bestimmter RFID-Chip vorgesehen ist, könnte eine Anwendungskennung (AK)[22] eingeführt werden. Um die mögliche Verwendung der Daten zu beschreiben, könnte zusätzlich eine Verwendungskennung (VK)[23] genutzt werden.[24] Beide Kennungen sind im Chip gespeichert und gegen Veränderung gesperrt. Bei einer Anfrage sendet das Lesegerät immer eine AK aus, die genau eine Anwendung spezifiziert. Ein RFID-Chip antwortet nur dann, wenn diese AK mit der eigenen Anwendungskennung übereinstimmt. Bei einer Antwort sendet der RFID-Chip seine ID und seine VK.

4.4 Zugriffsschutz

Zweckbindung kann auch durch einen Zugriffsschutz gesichert oder unterstützt werden, der den Zugriff jeweils nur dem berechtigten Nutzer der Daten ermöglicht. Um ihn zu realisieren, gibt es unterschiedliche Möglichkeiten, deren praktische Umsetzung bisher allerdings kaum über Laborexperimente hinaus kam.

4.4.1 Verschlüsselung der Daten

Eine klassische Methode der Zugriffssicherung ist, die Daten zu verschlüsseln und den Schlüssel nur dem Berechtigten zu geben. Dies stößt im Umfeld allgegenwärtiger Datenverarbeitung aller-

[22] Ein ähnliches Verfahren ist bereits in ISO/IEC 15693 in Form eines »Application Family Identifiers« (AFI) spezifiziert.

[23] Eine ähnliche Kennung ist bereits in ISO/IEC 15693 in Form eines »Data Storage Format Identifiers« (DSFID) vorgesehen.

[24] S. näher Müller/Handy, DuD 2004, 569; s. zu solchen Verfahren auch Flörkemeier/Schneider/Langheinrich 2004; BSI 2004, 54.

dings auf praktische Schwierigkeiten, weil die kleinen Chips und Sensoren oft nur sehr wenig Prozessorkapazität und vor allem wenig Energie zur Verfügung haben. Eine Verschlüsselung der Daten auf RFID-Chips oder der weiter zu meldenden Sensordaten kann den Energiebedarf vervielfachen und die verfügbare Energiekapazität übersteigen. Daher sind diese Daten in der Regel unverschlüsselt. Eine Verschlüsselung ist nur bei größeren Prozessoren mit ausreichender Energieversorgung möglich.[25]

4.4.2 Verschlüsselung der Identifikationsnummer

Einen anderen Schutz vor unerlaubtem Auslesen von RFID-Chips könnte erreicht werden, wenn nur die Identifikationsnummer verschlüsselt wird. Der Chip antwortet dann nicht mehr mit seiner originären Nummer, sondern mit einer »Meta-ID«, die aus der Verschlüsselung der Originalkennung entstanden ist. Die eigentliche Kennung erfährt nur derjenige, der den geheimen Schlüssel an den Chip sendet. Diese bildet aus dem empfangenen Schlüssel die dazugehörige Meta-ID und vergleicht diese mit der gespeicherten Meta-ID. Bei Gleichheit werden die Klardaten an das Lesegerät übertragen.[26]

Da jedoch das Verfolgen eines bestimmten Tags trotz Chiffrierung auch weiterhin möglich ist, wurde vorgeschlagen, den verschlüsselten Wert nach jedem Auslesevorgang entlang eines vom Schlüssel abhängigen Verfahrens zu ändern. Dadurch könnten legitime Besitzer des gekennzeichneten Gegenstands diesen weiterhin identifizieren, das unerlaubte Auslesen wäre dadurch jedoch nutzlos geworden.[27]

[25] S. z.B. Mattern 2003c, 32; Müller/Handy, DuD 2004, 656; Artikel-29-Datenschutzgruppe 2005a, 19f.; AK Technik 2006, 6; Fabian, in: TAUCIS 2006, 263f.; Voort/Ligtvoet 2006, 21.

[26] S. Sarma/Weis/Engels 2002, 454 ff.; Müller/Handy, DuD 2004, 658; Holznagel/Bonnekoh 2006, 42; Holznagel/Bonnekoh, MMR 2006, 23; Langheinrich 2006, 14; Fabian, in: TAUCIS 2006, 275 ff.

[27] S. z.B. Langheinrich 2007a, 135; BSI 2004, 53f.; s. hierzu und zu weiteren Möglichkeiten die Identität des Chips zu verschleiern Fabian, in: TAUCIS 2006, 278 ff.

Auch bei diesem Verfahren gestaltet sich die praktische Umsetzung schwierig. Ähnlich wie beim Kill-Befehl ist unklar, ob sich die für dieses Verfahren nötige soft- und hardwaretechnische Infrastruktur entlang komplexer Lieferketten und außerhalb von Einzelhandelskonzernen überhaupt ökonomisch und politisch durchsetzen lässt.[28] Um das Verfahren zu vereinfachen wird vorgeschlagen, auf Verschlüsselung zu verzichten und eine fixe Anzahl gespeicherter IDs in fester Reihenfolge zu verwenden.[29] Aber auch bei diesem Verfahren bleibt die Herausforderung, die zur Kontrolle des RFID-Tags nötigen Informationen entlang der Lieferkette bis zum Kunden zu übermitteln.[30]

4.4.3 Distanzbasierter Zugriffsschutz

Ein weiterer Ansatz steuert den Zugriff auf RFID-Daten in Abhängigkeit von der Entfernung zwischen Chip und Lesegerät.[31] Ein Lesegerät erhält umso mehr Informationen je näher es am Chip ist. Dabei messen RFID-Tags die Signalstärke des auslesenden Lesegeräts und geben in Abhängigkeit von dessen daraus ermittelter Distanz mehr oder weniger Details preis – bei großer Distanz beispielsweise lediglich die Präsenz eines Tags, bei größerer Nähe generische Klassenattribute (z.B. die Farbe) und beim geringsten Abstand schließlich die eindeutige ID.[32] Vorstellbar wäre auch eine Variante, bei der ein RFID-Chip aus großer, nur durch die Reichweite des RFID-Systems beschränkter, Entfernung auslesbar ist, jedoch Schreibzugriffe nur bei sehr geringem Abstand des Lesegeräts zum Chip zulässt. Das Nähe-Prinzip könnte außerdem mit Authentifizierungsverfahren kombiniert werden. Problematisch bei diesem Ansatz ist die Erkennung der Entfernung zwischen RFID-Chip und Lesegerät, da die empfan-

[28] Langheinrich 2005a, 356; Langheinrich 2007a, 136.

[29] Juels 2004.

[30] Langheinrich 2007a, 136: »utopisch«.

[31] Fishkin/Roy 2003.

[32] S. z.B. Langheinrich 2007a, 136; Langheinrich 2005a, 347f

gene Signalstärke von vielen Umgebungsbedingungen (wie Lage und Umhüllung des Chips) und dem Energieeinsatz abhängig ist.[33]

4.4.4 Blocker-Tags und Blocker-Token

Das unberechtigte Auslesen eines RFID-Chips kann durch einen Blocker-Tag unterbunden werden. Er stört diese Kommunikation nur dann, wenn das Lesegerät spezielle, als privat gekennzeichnete Kennungen abfragen will.[34] Im einfachsten Fall könnte der Adressraum von RFID-Chips in eine private und eine öffentliche Zone aufgeteilt sein. Die Kennung aller privaten Chips beginnt mit 0, alle Kennungen öffentlicher Verwendungen mit 1. Sobald ein Lesegerät versucht, im privaten Adressbereich nach RFID-Chips zu suchen, wird das Blocker-Tag aktiv und stört diesen Vorgang, indem es dem Lesegerät vorgaukelt, es wären Millionen von RFID-Chips vorhanden.[35] Das Lesegerät kann daraufhin real vorhandene RFID-Chips nicht mehr erkennen.[36] Diese Lösung erfordert jedoch, dass persönliche Gegenstände jeweils manuell in den geschützten Bereich ein- und ausgebucht werden. Auch unterliegt ein einfaches Blocker-Tag denselben Unwägbarkeiten wie reguläre RFID-Tags, das heißt, eine zu große Nähe zu einem metallischen Leiter könnte seinerseits das Blocker-Tag deaktivieren, wodurch sämtliche geschützten Tags plötzlich sichtbar würden.[37]

[33] S. Müller/Handy, DuD 2004, 658; Langheinrich 2007a, 136; Langheinrich 2005a, 347f.

[34] S. Juels/Rivest/Szydlo 2003, 103 ff.

[35] Dies kann bei zulässigen Lesevorgängen eine Ordnungswidrigkeit nach FTEG darstellen. Eine Strafbarkeit nach § 317 Abs. 1 StGB entfällt, weil RFID-Systeme nicht Teil von dem Betrieb öffentlichen Zwecken dienenden Telekommunikationsanlagen sind – s. näher Müller/Handy, DuD 2004, 68.

[36] S. z.B. Müller/Handy, DuD 2004, 658; BSI 2004, 53; Langheinrich 2005a, 350f.; AK Technik 2006, 15; Holznagel/Bonnekoh 2006, 42; Holznagel/Bonnekoh, MMR 2006, 23; Fabian, in: TAUCIS 2006, 269f.

[37] Langheinrich 2007, 137.

Diese Probleme ließen sich vermeiden, wenn ein mächtiges, batteriebetriebenes Gerät wie etwa ein Mobiltelefon den Schutz vor unautorisiertem Auslesen, sowie ein Kennwortmanagement zwecks Autorisierung und Abhörsicherung für alle mit sich geführten RFID-Tags anbieten kann. Durch die Auslagerung solcher Funktionen können diese nicht nur verlässlicher, sondern auch anspruchsvoller gestaltet werden. So könnte beispielsweise ein Blocker-Handy in Abhängigkeit vom Aufenthaltsort das Auslesen der eigenen RFID-Tags frei schalten: zum Beispiel Zuhause oder für die eigenen Schuhe, wenn man sich im Schuhgeschäft befindet.[38]

4.4.5 Verschlüsselung der Kommunikation

Werden Daten von oder zu kommunikationsfähigen Gegenständen übertragen, kann dies gegen unberechtigtes Abhören dadurch geschützt werden, dass die Übertragung verschlüsselt erfolgt.[39] So wird zum Beispiel der RFID-Chip mit biometrischen Merkmalen im neuen deutschen Reisepass verschlüsselt ausgelesen.[40] Bevor jedoch das Lesegerät einen RFID-Chip auslesen kann, muss dieser durch ein Anti-Kollisionsverfahren[41] eindeutig ausgewählt werden. Hierfür benötigt jeder RFID-Chip eine eindeutige ID, die nicht mit der »eigentlichen« ID identisch sein muss. Diese kann zwar vom Chip jedes Mal zufällig gewählt werden,[42] doch treibt diese Funktion die Herstellungskosten signifikant in die Höhe und wird deshalb in den meisten Fällen mit einer statischen ID erfüllt. Dadurch lassen sich Chips trotz Verschlüsselung wieder erkennen und daher über viele Stationen verfolgen.

[38] Juels/Syverson/Bailey 2005; Langheinrich 2006, 15; Langheinrich 2007a, 58.

[39] S. für Sensorknoten Fabian, in: TAUCIS 2006, 290f.

[40] S. hierzu näher Kügler, c't 2005 (5), 84 ff. und Kügler/Naumann, DuD 2007, 179f.; Hansen, in TAUCIS 2006, 264 ff.; s. allgemein BSI 2004, 50; Fabian, in: TAUCIS 2006, 275; Langheinrich 2007a, 137f.

[41] S. näher Langheinrich 2005a, 348 ff

[42] Dies ist in praktisch allen Standards von EPCglobal bereits vorgesehen, jedoch optional – s. Langheinrich 2007a, 137f.

Die Sicherung durch variable IDs und Verschlüsselung und das damit verbundene Kennwort-Management sind praktisch nur für »wertvolle« RFID-Chips realisierbar.[43]

4.5 Datensparsamkeit

Datensparsamkeit lässt sich zum einen dadurch erreichen, dass die Systeme allgegenwärtiger Datenverarbeitung so gestaltet werden, dass sie ohne personenbezogene Daten arbeiten können oder dass sie die personenbezogenen Daten nur sehr kurzfristig für das rein technische Erbringen der Dienstleistung erheben, verarbeiten und nutzen und danach sofort wieder löschen.[44] Zum anderen kann Datensparsamkeit dadurch erreicht werden, dass personenbezogene Daten anonymisiert oder pseudonymisiert werden.

4.5.1 Anonymisierung

Eine radikale Form der Anonymisierung ist das Deaktivieren des RFID-Tags durch einen Kill-Befehl.[45] Eine moderatere Form, die einige Funktionen des RFID-Tags noch erhält, ist ein modifizierter Kill-Befehl, der nur den eindeutig identifizierenden Teil der Kennung löscht. Dadurch entfällt die individualisierende ID des Gegenstands, die Bezeichnung der Objektklasse und weitere Daten bleiben jedoch für nachfolgende Anwendungen erhalten. Eine individuelle Zuordnung zu einem Nutzer ist über den Chip nicht mehr möglich. Will der Nutzer dies für seine Zwecke tun, kann er gegebenenfalls eine eigene Inventarnummer einsetzen.[46]

43 Langheinrich 2007a, 137.

44 Hieran schließt der Vorschlag einer gesonderten Regelung der Datenverarbeitung ohne gezielten Personenbezug an – s. unten 181 ff.

45 S. hierzu Langheinrich 2005a, 341 ff.

46 S. hierzu Müller/Handy, DuD 2004, 658.

Ein zweiter Gestaltungsvorschlag betrifft die Infrastruktur eines serverbasierten, überregional vernetzten RFID-Systems, wie es vom EPCglobal-Konsortium vorgeschlagen wird. Auf Anforderung des Nutzers sollte der informationelle Zusammenhang zwischen RFID-Tag und eindeutig identifizierbarem Gegenstand dadurch aufgelöst werden, dass der Eintrag im »Object Name Service (ONS)« (oder in einer vergleichbaren Datenbank eines anderen Systems) gelöscht oder zumindest gesperrt wird.[47] Dann lässt sich zwar weiterhin der RFID-Tag mit jedem Lesegerät auslesen, personenbezogene Daten können damit jedoch nicht erlangt werden. Alternativ könnte im Speicher des RFID-Tags ein Löschungsbit gesetzt werden. Registriert ein Lesegerät, das an das EPCglobal-Netzwerk angeschlossen ist, dieses Bit, so wird eine Löschung oder eine Sperrung des ONS-Eintrages veranlasst.[48]

4.5.2 Pseudonymisierung

Eine Form der Pseudonymisierung ist die Verwendung von Meta-IDs.[49] Diese sind für alle nicht berechtigten Nutzer Pseudonyme, die keinen Rückschluss auf die wahre ID und damit eventuell auf den Betroffenen ermöglichen, die aber bei Kenntnis des Schlüssels sich auflösen lassen und die wahre Identität des RFID-Tags preisgeben.[50] Bei gleich bleibender Meta-ID kann jedoch diese für die Verfolgung des Tags benutzt werden. Daher wurden mehrere Verfahren vorgeschlagen, wie diese Möglichkeit durch variable Meta-IDs vermieden werden kann.[51]

47 Diese Forderung lässt sich auf § 34 Abs. 2 bis Abs. 5 BDSG stützen.

48 S. hierzu Müller/Handy, DuD 2004, 659.

49 S. zu diesen bereits oben 166.

50 S. z.B. BSI 2004, 52; Langheinrich 2005a, 343f.

51 S. hierzu oben 166 sowie BSI 2004, 52f.; Langheinrich 2005a, 344 ff.; Fabian, in: TAUCIS 2006, 275 ff.

4.6 Datenschutz durch Technik

Für allgegenwärtige Datenverarbeitung – insbesondere für RFID-Anwendungen – gibt es eine Reihe von Techniken, die geeignet sind, die Durchsetzung von Grundsätzen des Datenschutzes zu unterstützen. Einige sind bereits realisiert, andere sind erst prototypisch umgesetzt oder bestehen nur als konzeptionelle Vorschläge. Für viele auf RFID bezogene Vorschläge gilt, dass sie durch relativ geringe Änderungen existierender Protokolle realisiert werden können.[52]

Die kurze Durchsicht der technischen Möglichkeiten hat aber auch gezeigt, dass einige datenschutztechnische Lösungen sehr voraussetzungsvoll sind, ein umfangreiches und kompliziertes organisatorisches Umfeld benötigen, zusätzliche – zum Teil nicht unbedeutende – Kosten verursachen, in ihrem Anwendungsfeld begrenzt sind, vom Betroffenen einen gewissen Aufwand erfordern und ihrerseits auch problematische Folgen haben können.[53] Viele von ihnen werden nur dann einsetzbar sein, wenn für sie ein geeigneter rechtlicher Rahmen geschaffen wird, der ihre Verwendung vorschreibt und ausgestaltet.

Für die folgenden Überlegungen ist zweierlei festzuhalten: Erstens ist Datenschutztechnik in der allgegenwärtigen Datenverarbeitung kein Selbstläufer, der durch eine unbeeinflusste technisch-wirtschaftliche Entwicklung dazu führt, dass die beschriebenen Datenschutzrisiken[54] vermieden oder deutlich reduziert oder die analysierten normativen Defizite[55] kompensiert werden. Wenn die Technik ihren möglichen Beitrag zur Gewährleistung von Datenschutz leisten soll, dann ist dies nur möglich, wenn diese Aufgabe und Zielsetzung von Anfang an bei der Entwicklung und Gestaltung, aber auch bei der Markteinführung

[52] BSI 2004, 54; Artikel-29-Datenschutzgruppe 2005a, 14.

[53] S. hierzu auch die Zusammenfassung von Langheinrich 2005a, 355 ff.; s. auch Fabian, in: TAUCIS 2006, 286 ff.

[54] S. oben 85 ff.

[55] S. oben 128 ff.

und der Anwendungsvorbereitung berücksichtigt wird.[56] Für ihre Verbreitung und Effektivität ist Datenschutztechnik auf Datenschutzrecht angewiesen.

Zweitens aber ist das Datenschutzrecht darauf angewiesen, dass es von der Technik unterstützt wird. Technische Vorschläge müssen Gestaltungsspielräume für rechtliche Regelungen schaffen. Es müssen technische Entwicklungen vorangetrieben werden, die gewährleisten, dass Grundsätze datenschutzgerechter Datenverarbeitung soweit wie möglich umsetzbar bleiben. Zugleich muss vermieden werden, dass die Technik allgegenwärtiger Datenverarbeitung so fortentwickelt wird, dass alle denkbaren Ansatzpunkte für Transparenz, Zweckbegrenzung, Kontrolle und Selbstbestimmung verloren gehen. Schließlich müssen technische Instrumente die Umsetzung von Recht in einem technischen Umfeld ermöglichen. Datenschutzrecht ist auf Datenschutztechnik angewiesen.

Zum Schutz der informationellen Selbstbestimmung müssen Recht und Technik eine Allianz eingehen.[57] Technik muss Recht unterstützen, seine Freiheits- und Schutzziele zu erreichen. Recht muss Technik unterstützen, damit Anreize für Technikentwicklungen geschaffen werden, die Aufwände und Kosten gerecht verteilt werden und Verantwortung an der richtigen Stelle eingefordert wird. Nur in diesem Zusammenspiel wird es möglich sein, informationelle Selbstbestimmung auch in einem informatisierten Alltag zur Geltung zu bringen.

Als erster Schritt hierzu ist erforderlich, dass das Datenschutzrecht modernisiert wird. Notwendig ist eine Anpassung des datenschutzrechtlichen Schutzprogramms an die Umsetzungsbedingungen in einer Welt allgegenwärtiger Datenverarbeitung, damit es nicht von der technischen Realität zur Bedeutungslosig-

[56] Weiser, Scientific American 1991, 75; BSI 2004, 110; Langheinrich 2005a, 340; Voort/Ligtvoet 2006, 18; Artikel-29-Datenschutzgruppe 2005a, 13.

[57] S. hierzu ausführlich Roßnagel 2001.

keit degradiert wird.[58] Um es auf die neuen Herausforderungen einzustellen, muss es risikogerecht fortentwickelt werden, und um es vollziehbar zu machen, muss es vereinfacht und in seinen Anforderungen handhabbar werden.

[58] Langheinrich 2005a, 340.

5. MODERNISIERUNG DES DATENSCHUTZRECHTS

Durch allgegenwärtige Datenverarbeitung wird das gegenwärtige Schutzprogramm, nicht aber die Notwendigkeit informationeller Selbstbestimmung in Frage gestellt. Wenn die Welt human und lebenswert sein soll, muss Selbstbestimmung mehr noch als heute gewährleistet sein. Informationelle Selbstbestimmung wird als normatives Konzept immer wichtiger, je größer die Risiken für die freie Entfaltung von Individuen und die demokratische Entwicklung der Gesellschaft durch eine Datenverarbeitung werden, die immer stärker in den alltäglichen Lebensvollzug eindringt und Angaben aus allen Lebensbereichen und Situationen aufnimmt und nutzt.

Allerdings muss das Schutzprogramm für dieses Grundrecht verändert und erweitert, letztlich den neuen Herausforderungen angepasst sein. Dies kann nicht dadurch geschehen, dass die Grundsätze des bisherigen Schutzprogramms vollständig aufgegeben werden. Denn sie sind ja aus der Zielsetzung der informationellen Selbstbestimmung abgeleitet. Erforderlich ist jedoch, die Konzepte und Instrumente des Datenschutzes der Allgegenwärtigkeit der Datenverarbeitung anzupassen. Wenn allgegenwärtige Datenverarbeitung überall, zu jeder Zeit, im Hintergrund und auf breite und vielfältige Infrastrukturen gestützt, automatisch, unbemerkt und beiläufig stattfindet, dann muss dies für den künftigen Datenschutz auch gelten. Selbstbestimmung muss überall und jederzeit möglich sein. Sie muss durch Infrastrukturen unterstützt werden, die ermöglichen auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt.

Die notwendige Fortentwicklung des Datenschutzrechts, die dies sicherstellt, kann nicht dadurch erreicht werden, dass für die

neuen Risiken ein weiteres, eigenes Datenschutzgesetz geschaffen wird. Dies würde das schwer verständliche Datenschutzrecht nur noch unübersichtlicher machen. Eine Fortentwicklung des Datenschutzrechts darf nicht nur an den Bedingungen der allgegenwärtigen Datenverarbeitung ausgerichtet werden, sondern muss in die Konzepte für eine Modernisierung des Datenschutzrechts eingebettet sein.[1] Notwendig ist daher eine umfassende Modernisierung des Datenschutzrechts, die dem Datenschutz insgesamt eine neue Struktur gibt, dabei aber angemessen auf die neuen Gefährdungen ausgerichtet ist.[2] Das heißt konkret: Ein fortentwickeltes Schutzprogramm soll nicht nur risikoadäquat sein, sondern muss das Datenschutzrecht auch noch einfacher und verständlicher machen.[3]

5.1 Konzepte notwendiger Modernisierung

Wie ein solches Schutzprogramm in der Modifikation und Ergänzung bisheriger Bestandteile aussehen könnte, soll abschließend angedeutet werden.[4] Hierfür sollen zehn Grundsätze vorgestellt werden, die in die Richtung der notwendigen Neuorientierung weisen.

5.1.1 Informationelle Selbstbestimmung durch »Opt-in«

Bisher wird die Erhebung, Verarbeitung und Nutzung personenbezogener Daten dadurch erlaubt, dass entweder der Gesetzgeber dies zulässt oder der Betroffene hierfür seine Einwilligung gibt. In der Praxis allgegenwärtiger Datenverarbeitung dürfte

1 S. Roßnagel/Pfitzmann/Garstka 2001. In diesem Gutachten zur Modernisierung des Datenschutzrechts wurden die Bedingungen der allgegenwärtigen Datenverarbeitung schon berücksichtigt – s. z.B. S. 15, 22f., 28, 42, 60, 63, 113 und 115.

2 S. Roßnagel, MMR 2005, 71 ff.

3 S. z.B. auch Simitis, DuD 2000, 714 ff.; Roßnagel/Pfitzmann/Garstka, DuD 2001, 253 ff.; Ahrend/Bijok u.a., DuD 2003, 433 ff.; Bizer, DuD 2004, 6 ff.; Tauss/Kollbeck/Fazlic 2004, 41.

4 S. hierzu auch Roßnagel, MMR 2005, 73 ff.; Roßnagel 2005a, 67 ff.

die Mehrzahl der Aktionen im Umgang mit personenbezogenen Daten auf die gesetzliche Generalklausel der »berechtigten Interessen« gestützt werden.[5] Zwar muss die verantwortliche Stelle prüfen, ob ein Grund für die Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung ihr berechtigtes Interesse überwiegt. In der Praxis wird die verantwortliche Stelle jedoch selten einen Grund für diese Annahme finden.[6] Wenn sie ausnahmsweise durch einen Widerspruch des Betroffenen doch auf ein schützwürdiges Interesse aufmerksam gemacht wird, dürfte sie im Regelfall ihr eigenes Interesse höher bewerten. Der weite Begriff der »berechtigten Interessen« ermöglicht so in der Praxis nahezu jede von der verantwortlichen Stelle gewünschte Datenverarbeitung.

Diese Regelung widerspricht dem verfassungsrechtlichen Konzept der Entscheidungsprärogative des Betroffenen. Dieses fordert, dem Betroffenen die Wahrnehmung seines Grundrechts auf informationelle Selbstbestimmung dadurch zu ermöglichen, dass die verantwortliche Stelle im Regelfall dessen Entscheidung abwartet und respektiert.[7] Die Entscheidungsbefugnis des Betroffenen anzuerkennen entspricht auch dem Grundmodell des Privatrechts: Die Rechte einer Privatperson gegenüber einer anderen können nicht über das hinausgehen, was diese ihr konkret zugestanden hat.[8] Die Grundlage für die Verarbeitung personenbezogener Daten kann daher im nicht öffentlichen Bereich grundsätzlich nur der freie Wille des Betroffenen sein. Als Grundsatz sollte daher auch für den Umgang mit personenbezogenen Daten – statt der beschränkten »Opt-out-Lösung« der »berechtigten Interessen« – eine »Opt-in-Lösung« gewählt werden.[9]

5 § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 3 Nr. 1 BDSG.

6 Eine Ausnahme dürften umfassende und tiefgehende Profile sein – s. z.B. Holznagel/Bonnekoh 2006, 34; Jandt/Laue, K&R 2006, 316 ff.

7 Roßnagel/Pfitzmann/Garstka 2001, 79.

8 S. auch Bizer, DuD 2001, 276f.; Roßnagel/Pfitzmann/Garstka 2001, 73.

9 Roßnagel/Pfitzmann/Garstka 2001, 73.

Diese grundsätzlich notwendige Reform des Datenschutzrechts ist in einer Welt allgegenwärtiger Datenverarbeitung besonders relevant, weil hier personenbezogene Daten alltäglich, in hoher Zahl, unmerklich, in komplexen Strukturen, oft ohne klare Zuordnung von Verantwortung erhoben und verarbeitet werden. In dieser Welt kann informationelle Selbstbestimmung nur noch in der Form von »Opt-in« wahrgenommen werden: »Opt-in« begründet eine Handlungspflicht des Verarbeiters. »Opt-in« bewirkt Datenschutz vor der Erhebung von Daten und wirkt dadurch präventiv. Der Betroffene wird mit dem Ansinnen der verantwortlichen Stelle konfrontiert und kann darauf reagieren. Ohne »Opt-in« des Betroffenen ist die Datenverarbeitung unzulässig. Für die Rechtmäßigkeit trägt der Datenverarbeiter die Nachweislast.[10]

Dagegen wirkt »Opt-out« nur im Nachhinein und korrigiert bestenfalls bereits erfolgte Datenerhebungen, -verarbeitungen und -nutzungen – soweit dies überhaupt möglich ist. »Opt-out« erfordert Initiativen des Betroffenen: Er muss den Umgang mit seinen Daten erkennen, ihn prüfen, den Verantwortlichen ausfindig machen und ihm gegenüber seine Forderung geltend machen. Dies ist unter den Umständen allgegenwärtiger Datenverarbeitung praktisch unmöglich. Zudem trägt er im Streitfall die Beweislast und damit ein erhöhtes Prozessrisiko. Eine »Opt-out-Lösung« führt unter den Bedingungen allgegenwärtiger Datenverarbeitung dazu, dass informationelle Selbstbestimmung praktisch abgeschafft ist.

Auch wenn eine »Opt-in-Lösung« erforderlich ist, bedeutet dies nicht, dass sie auch möglich ist. Die Untersuchung zur Wirksamkeit der Grundprinzipien des Datenschutzrechts[11] hat gezeigt, dass eine datenschutzrechtliche Einwilligung nach dem Modell des § 4a BDSG – von Ausnahmen abgesehen[12] – kaum noch zu

[10] Auch Thiesse 2005, 372 schlägt »Opt-in-Mechanismen« vor, um die Akzeptanz für RFID-Anwendungen beim Verbraucher zu erhöhen. Holznagel/Bonnekoh 2006, 30 ff. fordern ebenfalls beim RFID-Einsatz grundsätzlich eine Einwilligung.

[11] S. oben 136 ff. (3.4.3)

[12] S. oben 120 ff. (3.3.1)

verwirklichen ist. Wenn ein »Opt-in-Modell« für eine allgegenwärtige Datenverarbeitung realisiert werden soll, muss es erheblich modifiziert und den neuen Bedingungen angepasst werden.

Hierzu müsste es möglich sein, dass die Einwilligung auf ein technisches Gerät des Betroffenen »delegiert« werden kann. Dieses würde bei jedem signalisierten Verarbeitungsvorgang im Hintergrund die Datenschutzerklärungen überprüfen, akzeptieren oder verwerfen.[13] Dies setzt allerdings voraus, dass die Datenschutzpräferenzen zumindest für Normalfälle spezifizierbar sind. Hierfür könnten Datenschutzbeauftragte, Datenschutzvereinigungen, sonstige Verbände und Organisationen Empfehlungen in Form direkt einsetzbarer Präferenzmuster geben. Die Anforderungen an die Form der Einwilligung müssten den technischen Möglichkeiten angepasst werden.

Als ein »Opt-in« müsste auch anzusehen sein, wenn ein Betroffener bewusst und freiwillig seine individuellen Fähigkeiten unterstützende und verstärkende Techniksysteme und Dienste nutzt. Im Gegenzug müssten diese so gestaltet sein, dass sie über Datenschutzfunktionen verfügen, die er auswählen und für sich konfigurieren kann.[14]

5.1.2 Gestaltungs- und Verarbeitungsregeln

Bisher konzentriert sich Datenschutzrecht vor allem auf die Frage der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. Die Zulässigkeit hängt von einer gesetzlichen oder individuellen Erlaubnis ab. Dadurch wird das Interesse auf den Akt der Erlaubnis gelenkt. Diese ist aber ein einmaliger Akt, der zeitlich weit – oft Jahre und Jahrzehnte – vor der Datenverarbeitung liegt. Ihm liegt eine einmalige abstrakte Prüfung der Interessen zugrunde. Auf solche Zulassungsentscheidungen kann

[13] S. hierzu oben 161 ff. (4.2.).

[14] S. z.B. Schwenke 2006.

nicht verzichtet werden. Aber auf sie kann der Datenschutz nicht konzentriert werden. Wichtiger ist es, die konkreten und aktuellen Bedingungen des Umgangs mit den Daten zu berücksichtigen und die Art und Weise des Datenumgangs zu steuern. Daher könnten die Zulassungsregeln offener und genereller gefasst werden,[15] wenn die Beeinflussung des konkreten Umgangs mit den Daten stärker von der informationellen Selbstbestimmung beeinflusst werden könnten. Statt das Schwergewicht auf eine einmalige, abstrakte, vorlaufende und langfristig wirksame Zulassungsentscheidung durch die Zwecksetzung des Gesetzgebers oder des Betroffenen zu legen, sollte Datenschutz daher künftig vorrangig durch Gestaltungs- und Verarbeitungsregeln bewirkt werden, die permanent zu beachten sind.[16]

Solche Verarbeitungsregeln könnten zum Beispiel die Transparenz erhöhen. Diese könnte statt auf einzelne Daten stärker auf Strukturinformationen bezogen sein und statt durch eine einmalige Unterrichtung oder Benachrichtigung durch eine permanent einsehbare Datenschutzerklärung gewährleistet werden, die auf der »Homepage« des Gegenstands oder Systems einzusehen wäre. Eine andere Transparenzforderung könnte sein, – entsprechend dem Gedanken der §§ 6b Abs. 2 und 6c Abs. 3 BDSG – von allen datenverarbeitenden Alltagsgegenständen eine technisch auswertbare Signalisierung und Kennung zu fordern, wenn sie Daten erheben.[17] Diese könnten von »Datenschutzagenten« des Betroffenen verarbeitet werden. Im geeigneten Fall könnte auch eine aktuelle automatische Einwilligung erfolgen.[18]

Je stärker das Zusammenspiel zwischen enger Zwecksetzung und strenger Erforderlichkeit bei Gegenständen und Systemen an Grenzen stößt, die sich an den Nutzer anpassen, Aufgaben selbständig übernehmen oder sein Gedächtnis erweitern sollen, desto stärker muss das Datenschutzrecht die datensparsame Systemgestaltung in den Blick nehmen und Möglichkeiten sinnvollen anonymen und pseudonymen Handelns einfordern. Außerdem müssen in diesen Fällen Zweckbindung stärker auf Missbrauchsvermeidung und Erforderlichkeit stärker auf Löschungsregeln hin konzentriert werden. Die Umsetzung dieser Ziele sollten vor allem durch ein Datenschutzmanagementsystem erreicht werden, das auditiert werden kann.[19] Die verantwortliche Stelle sollte in ihrem Datenschutzkonzept nachweisen, dass sie die Gestaltungsziele erreicht hat.[20]

Vereinfacht und effektiviert würde der Datenschutz für viele Anwendungen der allgegenwärtigen Datenverarbeitung, wenn als zulässiger Zweck relativ weit das Erbringen einer rein technischen Funktion anerkannt, dafür aber als Ersatz die Verwendung der Daten strikt auf diese Funktion begrenzt würde. Dies könnte erreicht werden, wenn zwischen einer Datenverarbeitung mit und ohne gezielten Personenbezug unterschieden würde.[21]

Eine Datenverarbeitung ohne gezielten Personenbezug[22] betrifft die Verarbeitung personenbezogener Daten, die zur Erfüllung – vor allem technischer – Dienstleistungen technisch notwendig ist, ohne dass es dem Verarbeiter auf den Personenbezug ankommt.[23] Dies wird bei allgegenwärtiger Datenverarbeitung sehr oft der Fall sein. Sensoren erheben alle Veränderungen, die sie nach ihrer Fähigkeit erfassen können. Diese Daten werden nach

15 Dies würde die Kompliziertheit des Datenschutzrechts erheblich reduzieren.

16 S. Roßnagel/Pfitzmann/Garstka 2001, 70 ff.

17 S. hierzu näher oben 160 (4.1.1).

18 S. hierzu 161 (4.2) und 176 ff. (5.1.1).

19 S. näher unten 194 ff.

20 S. Roßnagel/Pfitzmann/Garstka 2001, 102.

21 S. näher Roßnagel/Pfitzmann/Garstka 2001, 68 ff., 113 ff.; Roßnagel 2006, 159.

22 Dieser Begriff wird nur für eine dogmatische Zusammenfassung der detailliert zu regelnden Tatbestandsvoraussetzungen benutzt – s. hierzu den Regelungsvorschlag in Roßnagel/Pfitzmann/Garstka 2001, 69.

23 Für diese Form der Datenverarbeitung im Rahmen der strategischen Telekommunikationskontrolle des BND stellt BVerfGE 100, 313 (366) fest: »An einem Eingriff fehlt es …, soweit Fernmeldevorgänge zwischen deutschen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden«; ebenso BVerfGE 107, 299 (328); BVerfG, NJW 2006, 1939 (1941), Rn. 74.

der Erhebung in der Form weiter verarbeitet,[24] dass sie mit anderen Sensordaten kombiniert und analysiert werden. Danach dürfte sich nur ein Bruchteil als interessant herausstellen. Die anderen Daten wurden nicht erhoben, um für sie einen Personenbezug herzustellen. Ähnlich verhält es sich mit dem Auslesen von RFID-Chips. Bei einer automatischen Erhebung werden unvermeidlich alle RFID-Chips in der Reichweite des Lesegeräts erfasst. Auch hier werden in einem weiteren Verarbeitungsschritt die relevanten von den nicht relevanten Daten getrennt. In Ad-Hoc-Netzen bilden sich die Kommunikationsverbindungen durch Peer-to-Peer-Kontakte zufällig Beteiligter. Um Telekommunikation zu ermöglichen, verarbeitet jeder personenbeziehbare Verkehrs-, Nutzungs- und Inhaltsdaten. Diese könnte er zwar zur Kenntnis nehmen, an ihnen hat er aber kein Interesse, weil er sie nur verarbeitet, um die Funktionen des Ad-Hoc-Netzes zu ermöglichen.

Die Anforderungen für diese Art der Datenverarbeitung sollten risikoadäquat und effizienzsteigernd spezifiziert werden.[25] Sie sollten insofern verschärft werden, als die Daten auf das erforderliche Minimum begrenzt, während ihrer Verarbeitung gegen Zweckentfremdung geschützt und nach der Verarbeitung sofort gelöscht werden müssen. Die Daten sollten außerdem einer strengen Zweckbindung (wie nach § 31 BDSG) unterliegen und durch ein Verwertungsverbot geschützt sein. Zur Unterstützung der Zweckbindung sollte ein Verstoß gegen sie in die Bußgeldvorschrift des § 43 BDSG aufgenommen werden. Werden diese Anforderungen nicht erfüllt, wird vor allem ein weitergehender

[24] Holznagel/Bonnekoh 2006, 62, weisen zwar zu Recht darauf hin, dass ein ungewolltes Auslesen keine Datenerhebung darstellt – s. auch Roßnagel/Pfitzmann/Garstka 2001, 70 –, verkennen aber, dass die Analyse und Bewertung Verarbeitungsvorgänge sein können, die unter das Datenschutzrecht fallen.

[25] Diesen Rechtsfolgenteil des Vorschlag ignorieren Möller/Bizer, in: TAUCIS 2006, 209 ff., in ihrer Kritik an der Unterscheidung von Daten mit und ohne gezieltem Personenbezug. Sie übersehen außerdem, dass dies ein rechtspolitischer Vorschlag – in einem neuen System mit neuen Definitionen und Rechtsfolgen – ist, und kein Vorschlag zu Interpretation von § 3 Nr. 1 BDSG.

Zweck mit diesen Daten verfolgt, sollten für sie von Anfang an alle Anforderungen für die Datenverarbeitung mit gezieltem Personenbezug gelten. Erleichterungen sollten insoweit vorgesehen werden, als auf eine vorherige Unterrichtung des Betroffenen verzichtet wird und ein Anspruch auf Auskunft über einzelne Daten für die kurze Zeit ihrer Speicherung nicht besteht, um kontraproduktive Protokollverfahren zu vermeiden. Die notwendige Transparenz sollte vielmehr durch eine veröffentlichte Datenschutzerklärung über die Struktur des Datenverarbeitungsverfahrens hergestellt werden.

5.1.3 Datenschutz durch Technik

Schon Mark Weiser hat 1991 darauf hingewiesen, dass Datenschutztechnik – von Anfang an im Design von Ubiquitous Computing-Systemen berücksichtigt – die informationelle Selbstbestimmung schützen und verhindern kann, dass schutzwürdige personenbezogene Daten bekannt werden. Eine gut gestaltete Form von Ubiquitous Computing könnte sogar besseren Datenschutz bieten als derzeit besteht.[26]

In einer durch und durch technisierten Welt hat Selbstbestimmung nur dann eine Chance, wenn sie technisch unterstützt wird.[27] Daher ist Datenschutzrecht auf Datenschutztechnik angewiesen. Und beide müssen den Anforderungen und Bedingungen des zu beeinflussenden Umfelds angemessen sein.[28]

Beispielsweise darf eine Kontrolle von Verarbeitungsregeln nicht eine permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen. Dies ist durch die bereits entwickelten oder konzipierten Transparenztechniken möglich.[29] Die Verwendung solcher Signalisierungs-, Identifizierungs- und

[26] Weiser, Scientific American 1991, 75.

[27] S. Köhntopp 2001, 55; Nedden 2001, 67.

[28] S. oben 172 ff. (4.6).

[29] S. zu diesen oben 159 ff.

Kommunikationsprotokolle müsste jedoch rechtlich gefordert werden, damit der Betroffene sicher sein kann, dass sein »Datenschutzagent« die Überprüfungen im Hintergrund durchführen und auch ausreichend informiert automatisch seine aktuellen Einwilligungen erteilen kann.

Selbst wenn die »verantwortlichen Stellen« – diese umfassen von einzelnen Personen bis zum großen Unternehmen eine sehr große Bandbreite von Akteuren – Datenschutzvorgaben einhalten wollen, sind ihnen oft nur die Funktionen der jeweiligen Anwendung, nicht aber die damit verbundenen Datenverarbeitungen bewusst und verständlich. Sie werden daher oft nicht in der Lage sein, die erforderlichen Datenschutzmaßnahmen zu gewährleisten, wenn diese nicht von Beginn an in der eingekauften Ubiquitous Computing-Technik eingebaut sind. Dies gilt umso mehr, je mächtiger die Informationstechnik ist, die – beispielsweise einem mit Wearable Computing aufgerüsteten Menschen[30] – zur Verfügung steht. Selbst bei gutem Willen haben sie ein Wissens- und Handlungsdefizit. Ohne eine entsprechende Vorinstallation der notwendigen Funktionen und ohne eine datenschutzfreundliche Konfiguration der Voreinstellungen sind sie kaum in der Lage, ihren Verpflichtungen zum Datenschutz nachzukommen.[31]

Die Durchsetzung von Verarbeitungsregeln muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erfolgen. Zum einen muss der Systemdatenschutz dazu führen, dass – soweit möglich – die technischen Systeme nur das können, was sie dürfen. Zum anderen müssen Endgeräte des Betroffenen in der Lage sein, die Datenerfassung durch fremde Geräte zu erkennen, zu beeinflussen,[32] nach den Präferenzen des Nutzers Kommunikation zu ermöglichen oder abzublocken,[33] Pseudonyme und andere Identitäten zu wechseln und zu verwalten,[34] Datenweitergaben zu protokollieren und Löschungsrechte automatisch geltend zu machen.

Technischer Datenschutz hat gegenüber rein rechtlichem Datenschutz gewisse 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.

Datenschutzrecht muss daher die Voraussetzungen für einen Datenschutz durch Technik schaffen.[35] Es muss Pflichten generieren oder Anreize schaffen, die Techniken zur Transparenz der Datenverarbeitung, zur technischen Ermöglichung von Einwilligungen, zur Markierung und Prüfung von Verarbeitungszwecken, zum Zugriffsschutz und zur Datensparsamkeit einzusetzen.[36] Unter Umständen muss es auch weitere Rahmenbedingungen regeln, die Voraussetzungen und Folgen der Techniknutzung betreffen.[37]

5.1.4 Vorsorgeregelungen

Wie in anderen Rechtsbereichen auch muss Vorsorge die Gefahrenabwehr ergänzen. Vorsorge könnte eine zweifache Ausprägung annehmen: zum einen die Reduzierung von Risiken und zum anderen präventive Folgenbegrenzungen potenzieller Schäden.

Die Risiken für 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

30 S. hierzu oben 69 f.

31 S. auch Artikel-29-Datenschutzgruppe 2005a, 13; s. für die IT-Sicherheit auch Möller/Bizer, in: TAUCIS 2006, 120.

32 S. Roßnagel/Müller, CR 2004, 629; Langheinrich 2005a, 347 ff.; Thiesse 2005. 371f.

33 S. Müller/Handy, DuD 2004, 655.

34 S. z.B. Möller, DuD 2006, 98 ff.; Hansen/Krasemann/Rost/Genghini, DuD 2003, 551 sowie für RFID Langheinrich 2005a, 343 ff., 358.

35 S. Roßnagel/Pfitzmann/Garstka 2001, 184.

36 Zu den Techniken s. 158 ff.

37 S. z.B. 188 ff. (Anreize), 191 ff. (Hersteller) und 194 ff. (Architektur)

noch keine personenbezogenen Daten entstanden sind oder verarbeitet werden.[38]

Mangels Personenbezug beim Erheben können beispielsweise Sensorinformationen, Umgebungsdaten oder RFID-Kennungen ohne Bindung an Datenschutzregeln erhoben und verarbeitet werden. Dies erlaubt auch Daten auf Vorrat zu sammeln, Präferenzen oder Verhaltensweisen zu einem Pseudonym zu beobachten und zu speichern und sogar umfassende pseudonyme Nutzerprofile anzulegen.[39] Auch wenn der Personenbezug bei Erhebung fehlt, kann dieser in der Folge aufgrund unterschiedlicher Gründe hergestellt werden. Gerade bei allgegenwärtiger Datenverarbeitung entstehen so viele Daten über den Kontext anderer Daten, dass durch das nachträgliche Erlangen von Zusatzwissen der Personenbezug zufällig oder absichtlich hergestellt werden kann. Auch kann der Betroffene den Bezug bewusst oder zufällig aufdecken.[40] Kommt es aber zur Herstellung des Personenbezugs, gilt dies meist nicht für *ein* Datum, sondern mit einem Schlag für *alle* zu dieser Person gespeicherten Angaben.[41] Dann aber können viele Schutzmaßnahmen, die das Datenschutzrecht für die Verarbeitung personenbezogener Daten fordert, die aber bisher unterbleiben konnten, nicht mehr sinnvoll nachgeholt werden.[42] Hier besteht das Risiko irreparabler Schäden und damit eine Schutzlücke für das Grundrecht auf informationelle Selbstbestimmung. Solche Daten erfordern vorsorgende Regelungen, wenn die Möglichkeit oder gar die Absicht besteht, sie irgendwann einmal mit einem Personenbezug zu versehen.[43]

[38] S. hierzu Roßnagel/Scholz, MMR 2000, 728 ff.; Roßnagel/Pfitzmann/Garstka 2001, 107 ff.; Müller 2007.

[39] S. hierzu Roßnagel/Scholz, MMR 2000, 721 ff.

[40] Zu weiteren möglichen Gründen s. Roßnagel/Pfitzmann/Garstka 2001, 107.

[41] S. näher Roßnagel/Scholz, MMR 2000, 729.

[42] Zu den Rechtsfolgen einer nachträglichen Aufdeckung eines Pseudonyms s. näher Roßnagel/Scholz, MMR 2000, 730.

[43] S. hierzu näher Roßnagel/Scholz, MMR 2000, 728 ff.; Roßnagel/Pfitzmann/Garstka 2001, 107 ff.; Müller 2007; ähnlich auch Möller/Bizer, in: TAUCIS 2006, 210.

Für diese potenziell personenbeziehbaren Daten den Begriff der personenbezogenen Daten auszuweiten, würde die relativ klare Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten aufweichen und würde in vielen Fällen auch zu unverhältnismäßigen Folgen führen. Aber auch der Vorschlag, die Personenbeziehbarkeit zu vermuten, wenn nicht die verantwortliche Stelle diese ausschließen kann,[44] ist keine geeignete Lösung, weil unklar bleibt, welche Datenschutzregelungen gelten sollen. Viele Datenschutzregelungen sind auf Daten, deren Betroffener unbekannt ist, nicht anzuwenden.

Notwendig ist eine spezifische Vorsorgeregelung[45] für potenziell personenbeziehbare Daten, die ein hohes Risikopotenzial beinhalten. Sie sollte das Ziel verfolgen, die Wahrscheinlichkeit der Personenbeziehbarkeit zu vermindern und das Schadenspotenzial einer Aufdeckung zu reduzieren. Hierzu könnte zum Beispiel für pseudonyme Profile[46] oder nicht personenbezogene Datensammlungen auf Vorrat gefordert werden, dass die nachträgliche Herstellung des Personenbezugs unzulässig ist und dass die Sammlungen nur an Dritte übermittelt werden dürfen, wenn sichergestellt ist, dass diese keinen Personenbezug herstellen können. Dies würde auch das Problem lösen, dass solche Daten in Europa erhoben, in »unsichere Drittstaaten« transferiert und dort – ohne Datenschutz – ausgewertet werden.[47]

Auch sind zur Risikobegrenzung Anforderungen an eine transparente, datensparsame, kontrollierbare und missbrauchsvermeidende Technikgestaltung zu formulieren. Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme

[44] So der Vorschlag von Möller/Bizer, in: TAUCIS 2006, 224.

[45] S. zu einem Formulierungsvorschlag Roßnagel/Pfitzmann/Garstka 2001, 110f.

[46] Für diese gilt auch das Verbot umfassender Profilierung. Nach BVerfGE 65, 1 (53), ist »eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen … *auch in der Anonymität* statistischer Erhebungen unzulässig«.

[47] Zu weiteren Vorsorgemaßnahmen s. Müller 2007.

präventiven (freiwilligen) Prüfungen ihrer Datenschutzkonformität zu unterziehen und diese Prüfung zu dokumentieren.[48]

5.1.5 Freiheitsfördernde Architekturen

Die Möglichkeiten der Überwachung und Kontrolle sind zum einen stark davon abhängig, Daten aus vielen Lebensbereichen zusammenführen zu können. Durch Anwendungen allgegenwärtiger Datenverarbeitung, die den gesamten Lebensalltag begleiten und das gesamte Geschehen zu Hause oder im Büro erfassen, entstehen nahezu vollständige Protokolle des Alltags. Aus diesen können leicht umfassende Profile der Bewegungen, Kontakte, Interessen, Präferenzen und Beziehungen einer Person erstellt werden.[49] Zum anderen setzen Überwachung und Kontrolle voraus, dass die daran Interessierten auf diese Daten – möglichst aktuell – zugreifen und sie für ihre Zwecke ausnutzen können.

Die Möglichkeiten der Überwachung und Kontrolle hängen entscheidend davon ab, wie die Architektur allgegenwärtiger Datenverarbeitung gestaltet und wie die Datenflüsse und -zugriffsmöglichkeiten organisiert sind. Da moderne Gesellschaften hochgradig arbeitsteilig organisiert und sehr differenziert gegliedert sind, bestehen und entstehen vielfältige, von einander unabhängige und oft sogar konkurrierende Datenverarbeitungsstrukturen. Die dadurch bestehende informationelle Gewaltenteilung erschwert rollenübergreifende Zusammenführungen von Daten und schützt dadurch die informationelle Selbstbestimmung. Dies belässt dem Betroffenen noch Möglichkeiten, in anderen sozialen Rollen selbst Informationen über sich preiszugeben, seine Selbstdarstellung zu kontrollieren und seine Persönlichkeit rollenübergreifend zu entwickeln. In einem solchen sozialen Umfeld hat auch ein intuitives oder technisch unterstütztes Identitätsmanagement gewisse Chancen, die personenbezogenen

[48] S. hierzu näher Roßnagel/Pfitzmann/Garstka 2001, 130 ff.

[49] S. oben 96 (Risiken).

Daten hinsichtlich der unterschiedlichen sozialen Rollen des Betroffenen zu verwalten.[50]

Der Schutz durch informationelle Gewaltenteilung geht jedoch verloren, wenn in den differenzierten Strukturen Daten rollenübergreifend erhoben, aus verschiedenen Lebensbereichen zusammengeführt oder für Dritte – eventuell sogar auf dem freien Markt – verfügbar gemacht werden. Dieses Risiko ist beim Zugriff der Strafverfolgungsbehörden und Nachrichtendienste auf diese Infrastrukturen besonders groß.[51] Sie können letztlich auf nahezu alle Informationsinfrastrukturen in der Gesellschaft zugreifen. Nicht nur der Umfang von Zugriffen wurde zunehmend ausgeweitet, sondern auch ihre Voraussetzungen immer wieder reduziert. Sie erfordern vielfach nicht mehr eine Straftat, eine Gefahr oder einen Verdacht. Sie sind inzwischen auch weit in deren Vorfeld zur Beobachtung oder zur Vorsorge hinsichtlich kritischer Entwicklungen zulässig. Die Überwachungsbehörden sind damit diejenige Instanz, die am ehesten in der Lage sind, potenziell alle Daten zu einer Person zusammen zu führen und daraus alle sozialen Rollen integrierende, die jeweilige Persönlichkeit intensiv repräsentierende Profile zu erstellen. Der neueste Schritt in diese Richtung ist die Vorratsspeicherung von Kommunikationsdaten, die nach der EG-Richtlinie 2006/24/EG eingeführt werden muss.[52]

Für die infrastrukturelle Ausgestaltung allgegenwärtiger Datenverarbeitung ist zum einen darauf zu achten, dass soweit wie möglich informationelle Gewaltenteilung realisiert wird. Zum anderen muss versucht werden, die Nützlichkeit allgegenwärtiger Datenverarbeitung von ihrem Kontrollpotenzial zu trennen. Drittens ist ein der allgegenwärtigen Datenverarbeitung angemessener Ausgleich der konfligierenden Interessen zwischen innerer Sicherheit und Grundrechtsschutz zu suchen. Einschränkungen

[50] S. Roßnagel, WI 2007, 13; zu Identitätsmanagement in der allgegenwärtigen Datenverarbeitung s. z.B. Hansen, in TAUCIS 2006, 310 ff.

[51] S. näher Roßnagel 2003e.

[52] S. hierzu Roßnagel, EuZ 2006, 30 ff.

der Grundrechte sind – wo immer möglich – als Ausnahmefall zu konzipieren und dürfen nicht den Alltag bestimmen. Vor allem im Vorfeld von Gefahren, wo es nur um Risikovorsorge geht, müssen Freiheitseingriffe Ausnahmen bleiben. Sie müssen kontrollierbar und begrenzbar sein. Diese Unterscheidung zwischen Normalität und Ausnahme gibt auch ein brauchbares Kriterium für die künftige Gestaltung der Infrastrukturarchitekturen.[53]

Diese sind am normalen Alltag und nicht am seltenen Extremfall zu orientieren. Allgegenwärtige Datenverarbeitung sollte den vielfältigen Bedürfnissen des Alltags gerecht werden, nicht aber vorrangig den seltenen Überwachungsinteressen. In der Alltagsnormalität muss der Grundrechtsschutz der Bürger Vorrang haben. Sie müssen Instrumente für eine sichere und vertrauenswürdige Kommunikation nutzen können und die Möglichkeit haben, ihrem Grundrecht auf informationelle Selbstbestimmung Wirksamkeit zu verschaffen. Der Normalfall darf daher nicht vom Interesse an einer massenhaften Datenbevorratung für den Ausnahmefall geprägt sein. Vor allem muss verhindert werden, dass in der Gesellschaft Strukturen verfestigt werden, die für »immer« überwachungsstaatliche Entwicklungen ermöglichen oder nahe legen.

Für den Ausnahmefall sind effektive Befugnisse zu schaffen, um aktuell, punktuell und auf Täter und Verdächtige sowie ihre Ressourcen bezogen schnell reagieren zu können. Statt massenhafter Auswertung von Daten aus Alltagsanwendungen ist zu versuchen, individuelle Überwachungsmaßnahmen an der »Quelle« und der »Senke« der Kommunikation Verdächtiger anzusetzen. Hilfsmittel hierfür reichen von der Aufzeichnung und Auswertung der elektromagnetischen Abstrahlung von Endgeräten bis hin zur Installation von Abhörtechnik. Die unvermeidlich weitgehenden Machtbefugnisse sollten aber jeweils auf den Ausnahmefall begrenzt, zeitlich befristet und kontrolliert sein.

[53] S. hierzu umfassend Roßnagel 2003e; für Telematikinfrastrukturen Roßnagel, NVZ 2006, 287f.

Im Rahmen der Architekturgestaltung muss auch berücksichtigt werden, dass es Räume und Zeiten gibt, in denen keine Datenerhebung stattfindet, die frei von Ubiquitous Computing sind. Rechtlich muss gewährleistet werden, dass es für allgegenwärtige Datenverarbeitung keinen »Anschluss- und Benutzungszwang« gibt.[54] Auch muss ein Kopplungsverbot sicherstellen, dass bestimmte wichtige Infrastrukturleistungen nicht davon abhängig gemacht werden dürfen, dass der Betroffene in die Erhebung von Daten, die nicht für die Funktionserfüllung unbedingt erforderlich sind, einwilligt.[55] Schließlich sollte in Form von Vorsorgeregelungen in bestimmten Bereichen sichergestellt werden, dass von allgegenwärtiger Datenverarbeitung freie Alternativen im Angebot von Diensten offen gehalten werden. Schließlich müsste die Aufgabe der datensparsamen oder datenvermeidenden Systemgestaltung nach § 3a BDSG aufgewertet und ihre Berücksichtigung bei der Gestaltung von IT-Architekturen überprüfbar werden.

5.1.6 Neue Regelungsadressaten

Hinsichtlich der Regelungsadressaten ist die zunehmende Verantwortungsdiffusion zur Kenntnis zu nehmen. An der Datenverarbeitung sind oft viele Akteure mit spontanen, kurzfristigen Aktionen beteiligt, die in ihrem – vielleicht nicht intendierten – Zusammenwirken erst die zu gestaltenden Wirkungen verursachen. Zwischen Datenverarbeitern und Betroffenen findet ein permanenter Rollenwechsel statt. Bei einzelnen Nutzern wächst die Kapazität zur Datenerhebung und -verarbeitung extrem, ohne dass dies auch nur annähernd für die Kenntnisse und Aufmerksamkeiten für die Eingriffe in Grundrechte anderer gilt. Regelungen, die sich nur an »verantwortliche Stellen« richten, dürften viele Gestaltungsziele nicht erreichen. Auch dürfen tech-

[54] Hierzu gehört auch das Recht, einen RFID-Chip an eigenen Gegenständen funktionsunfähig machen zu können – s. z.B. Artikel-29-Datenschutzgruppe 2005a, 17f.; Artikel-29-Datenschutzgruppe 2005b, 3.

[55] So für Telemedien nach § 12 Abs. 3 TMG.

nische Verfahren zur Gewährleistung von Datenschutz nicht nur beim Betroffenen ansetzten[56] und diesem den Aufwand und die Kosten aufbürden.

In viel stärkerem Maß sind daher künftig die Technikentwickler und -gestalter als Regelungsadressaten anzusprechen.[57] Viele Gestaltungsanforderungen können von den »verantwortlichen Stellen« gar nicht erfüllt werden.[58] Ihnen fehlen meist das technische Wissen, die Gestaltungskompetenz und vor allem der (legale) Zugriff auf Hard- und Software. In einer Welt allgegenwärtiger Datenverarbeitung wird vielfach Datenschutz nur noch zu realisieren sein, wenn er in technische Protokolle integriert[59] und in datenschutzkonforme Systementwürfe aufgenommen ist.[60] Statt Regelungsadressaten ohne Einfluss zu wählen, sollten diejenigen verpflichtet werden, die auch die entsprechenden Handlungsmöglichkeiten haben.

Die Technikentwickler und -gestalter sollten dazu angehalten werden zu prüfen, ob ihre Produkte datenschutzkonform gestaltet sind, diese Prüfungen zumindest für bestimmte Systeme zu dokumentieren und auf verbleibende Risiken hinzuweisen.[61] Auch sollten sie ihre Produkte mit datenschutzkonformen Defaulteinstellungen ausliefern.[62]

5.1.7 Einbezug privater Datenverarbeitung

Zur Erweiterung der Sinne, zur Verstärkung des Gedächtnisses, zur Befreiung von lästiger Arbeit oder zur Gewährleistung von Sicherheit können die Nutzer allgegenwärtiger Datenverarbeitung vielfältige Daten über andere Menschen in nahezu unbe-

[56] Dieses tun die meisten der oben 158 ff. vorgestellten Datenschutztechniken.
[57] S. hierzu Langheinrich 2005a, 357.
[58] S. auch oben 183 ff. (5.2.3).
[59] Langheinrich 2005a, 358.
[60] S. BSI 2006, 59, 65.
[61] S. näher Roßnagel/Pfitzmann/Garstka 2001, 143 ff.
[62] S. Roßnagel 2001, 24.

grenztem Umfang frei von allen datenschutzrechtlichen Vorgaben erheben, verarbeiten und nutzen, soweit dies persönlichen oder familiären Tätigkeiten dient.[63]

Aber bis wohin kann diese Ausnahme von der Geltung des Datenschutzrechts angesichts der zunehmenden informationstechnischen »Aufrüstung« des Einzelnen reichen? Schon heute verfügt er in seinem Auto über mehr als 100 Computer. Allein in seinem Laptop, seinem PDA und seinem Mobiltelefon trägt er mehr Rechenkapazität mit sich herum, als zur Entstehungszeit des Bundesdatenschutzgesetzes in eine Turnhalle gepasst hat. Diese Aufrüstung verdoppelt sich nicht nur hinsichtlich der Kapazität der Datenspeicherung, -verarbeitung und -übermittlung spätestens alle zwei Jahre,[64] sondern wird vor allem hinsichtlich der Fähigkeit, vielfältigste Daten automatisch zu erheben noch erheblich gesteigert. Alle Formen von Sensoren versetzen den Einzelnen in die Lage, ohne sein Zutun seine gesamte Umgebung in vielfältiger Hinsicht rund um die Uhr aufzunehmen und die Daten nach beliebigen Zwecken auszuwerten und zu nutzen.

In einer solchen Welt haben sich die Grundlagen, die zur Privilegierung der persönlichen und familiären Datenverarbeitung geführt haben, vollständig verändert. Angesichts des Risikopotenzials der privaten allgegenwärtigen Datenverarbeitung ist eine vollständige Ausnahme von der Geltung des Datenschutzrechts nicht mehr zu rechtfertigen.

Die zwar technisch aufgerüstete, aber immer noch private oder familiäre Datenverarbeitung sollte nicht vollständig dem Datenschutzrecht unterworfen werden. Dies dürfte vielfach zu unverhältnismäßigen Folgen führen.[65] Vielmehr sollte danach gesucht werden, welche Einzelregelungen Anwendung finden sollten, um das beispielsweise durch Wearable Computing verursachte Risiko für die informationelle Selbstbestimmung anderer zu

[63] S. hierzu oben 131 f.
[64] S. oben 26 f.
[65] S. Dammann/Simitis 1997, Einleitung Rn. 22.

beherrschen. Hierzu sollten zum Beispiel die Regelungen zum Datengeheimnis (§ 5 BDSG), zum Schadensersatz (§ 7 BDSG), zur Datensicherung (§ 9 BDSG) und zur Datenverarbeitung im Auftrag (§ 11 BDSG) gehören. Außerdem sollten angepasste Regelungen zur Signalisierung und Identifizierung sowie zur Auskunft vorgesehen werden.[66]

5.1.8 Anreize und Belohnungen

Die datenschutzgerechte Gestaltung der künftigen Welt allgegenwärtiger Datenverarbeitung ist durch herkömmliche Command-and-Control-Ansätze nicht zu erreichen. Sie fordert die aktive Mitwirkung der Entwickler, Gestalter, Anwender und Nutzer. Sie werden nur für eine Unterstützung zu gewinnen sein, wenn sie davon einen Vorteil haben. Daher sollte die Verfolgung legitimen Eigennutzes in einer Form ermöglicht werden, die zugleich auch Gemeinwohlbelangen dient. Datenschutz muss daher zu einem Werbeargument und Wettbewerbsvorteil werden.[67]

Außerdem sollten ordnungsrechtliche Regelungen nur erfolgen, wenn der Markt nicht von sich aus zu einer ausreichenden Verteilung datenschutzgerechter Technik führt. Wenn es gelingt, am Markt datenschutzgerechte Technik zu platzieren und attraktiv zu machen, kann die jeweils dynamische Reaktion der Anbieter von Datenschutztechnik auf die immer wieder neuen Risiken allgegenwärtiger Datenverarbeitung dazu führen, dass die Datenschutztechnik mit dem Entstehen neuer Risiken Schritt hält – viel eher jedenfalls, als der Gesetzgeber dies kann. Wenn sich

[66] Dass die Datenschutzrichtlinie die Datenverarbeitung, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher und familiärer Tätigkeiten vorgenommen wird, in Art. 3 Abs. 2 zweiter Anstrich von ihrer Anwendung ausschließt – s. Dammann/Simitis 1997, Art. 3 Rn. 7 – , behindert solche Regelungen nicht. Die Mitgliedstaaten sind frei, außerhalb des harmonisierten Anwendungsbereichs weitere Datenschutzregelungen zu treffen. Außerdem behindert die Richtlinie nicht die Fortentwicklung des Datenschutzrechts – s. Dammann/Simitis 1997, Einleitung Rn. 9f.; Roßnagel/Pfitzmann/Garstka 2001, 55 ff.

[67] S. für RFID Thiesse 2005, 372 ff.

Datenschutztechnik verkauft, wird sie sich immer wieder ebenso dynamisch entwickeln wie neue technische Herausforderungen für den Datenschutz.

Um für das Angebot datenschutzgerechter Technik und Anwendungen einen Markt zu schaffen und zu erhalten, ist eine vertrauenswürdige Information der Nutzer über technische Produkte und Anwendungen erforderlich. Hierfür kann das Recht die geeigneten Rahmenbedingungen schaffen, indem es für solche Technikprodukte Zertifikate[68] und für Anwendungen und Dienste ein freiwilliges Datenschutzaudit anbietet.[69] Datenschutzzertifikat und Datenschutzaudit geben dem Markt die erforderlichen Signale, dass hier jeweils Datenschutz in ausreichendem Maß gewahrt wird, und unterstützen so eine datenschutzbewusste Kaufentscheidung.

Wettbewerbsvorteile und Marktinformationen können durch die Präsentation eines Auditzeichens, eines Zertifikats oder einer Datenschutzerklärungen erreicht werden. Werden diese von Datenschutzempfehlungen à la »Stiftung Warentest«, von Datenschutzrankings oder durch die Berücksichtigung von Auditzeichen oder Zertifikaten bei der öffentlichen Auftragsvergabe begleitet, kann ein Wettbewerb um den besseren Datenschutz entstehen. Dann werden die Gestaltungsziele beinahe von selbst erreicht.[70]

Hier könnten auch Datenschutzbeauftragte und Datenschutzverbände eine neue Rolle finden, indem sie den Schwerpunkt ihrer Praxis von einer repressiven Kontrolle zu einer konstruktiven Unterstützung von Datenschutz verlegen. Sie erhielten ein ganz neues Image, wenn sie Empfehlungen aussprechen, Beratungen durchführen, Best Practice-Beispiele publizieren und Preise für gute Datenschutzlösungen vergeben.[71]

[68] S. z.B. Schläger, DuD 2004, 459, Bäumler, DuD 2004, 80; Bäumler, DuD 2002, 325; Bizer, DuD 2006, 5 ff.

[69] S. z.B. Roßnagel 2000; Roßnagel 2003d, 439 ff.

[70] S. hierzu ausführlich Roßnagel 2000, 3 ff.; Roßnagel 2002b, 131 ff.; Bäumler/v. Mutius 2002.

[71] S. z.B. Weichert 1998, 213 ff.

5.1.9 Gefährdungshaftung

Zusätzliche Anreize für die korrekte Einhaltung von Datenschutzregelungen können auch von dem Wunsch ausgehen, Schadensersatzzahlungen zu vermeiden. Von einer Haftungsregelung kann dann eine präventive Wirkung erwartet werden, wenn das Haftungsrisiko geringer wird oder gar entfällt, wenn die verantwortliche Stelle die datenschutzrechtlichen Pflichten nachweisbar vollständig erfüllt.

Zugleich haben Schadensersatzregelungen eine Ausgleichsfunktion. Diese wird aber nur erfüllt, wenn hierfür die Hürden nicht zu hoch sind. Will jedoch ein Geschädigter einen Schaden durch Datenverarbeitung geltend machen, besteht für ihn das grundsätzliche Problem, dass es nahezu unmöglich ist, sowohl die Ursächlichkeit als auch das Verschulden nachzuweisen. Dieses Problem wird bei einer allgegenwärtigen Datenverarbeitung noch erheblich verschärft, weil die Strukturen und Prozesse erheblich komplexer und dynamischer und für den Betroffenen noch weniger transparent sind.

Um das Problem zu mildern, regelt das Bundesdatenschutzgesetz in § 8 für den öffentlichen Bereich eine Gefährdungshaftung. Für den nicht öffentlichen Bereich sieht es dagegen in § 7 nur eine Verschuldenshaftung mit Beweislastumkehr vor. Sie entfällt, wenn die verantwortliche Stelle die nach den Umständen des Falls gebotene Sorgfalt beachtet hat.

Schon heute ist diese Differenzierung nicht einzusehen, da von der Datenverarbeitung im nicht öffentlichen Bereich mindestens das gleiche Schadensrisiko ausgeht wie im öffentlichen Bereich. In beiden ist die Grundlage der Gefährdungshaftung gleichermaßen gegeben, nämlich – wie allgemein im Recht – der Einsatz einer zwar erlaubten, aber gleichwohl gefährlichen Technik. Die Begründung für § 8 BDSG gilt ebenso für den nicht öffentlichen Bereich: »In Anbetracht der komplexen, für außenstehende Dritte kaum nachvollziehbaren Vorgänge bei der automatisierten Datenverarbeitung kann es dem Betroffenen nicht zugemutet werden, dem Betreiber der Anlage ein Verschulden nachweisen zu müssen.«[72] Diese Differenzierung ist im Zeitalter allgegenwärtiger Datenverarbeitung noch viel weniger nachzuvollziehen.

Angesichts der gegenwärtigen und zukünftigen Risiken für die informationelle Selbstbestimmung, erscheint eine Privilegierung privatwirtschaftlicher verantwortlicher Stellen nicht sachgerecht. Daher sollte eine Gefährdungshaftung für jede geschäftsmäßige automatisierte Datenverarbeitung gelten.[73] Für die Gefährdungshaftung ist eine Haftungshöchstgrenze vorzusehen und bis zu deren Höhe eine Deckungsvorsorge zu fordern. Um die strukturell bedingten Beweisprobleme des Geschädigten zu vermindern,[74] sollte das Gesetz außerdem eine Beweiserleichterung bieten:[75] Wenn der Geschädigte die Rechtswidrigkeit oder Unrichtigkeit der Datenverarbeitung sowie Umstände des Einzelfalls belegt, die eine hohe Wahrscheinlichkeit für die Ursächlichkeit des entstandenen Schadens begründen, soll die verantwortliche Stelle nachweisen müssen, dass ihr Fehler den Schaden nicht verursacht haben kann.[76]

Um den Vollzug der Datenschutzregelungen zu unterstützen, sollte jedoch die Gefährdungshaftung entfallen und an ihre Stelle die allgemeine Haftungsregelung treten, wenn die verantwortliche Stelle nachweist, dass sie für den Zeitraum, in dem die Regelverletzung erfolgt sein kann, alle Anforderungen des Datenschutzmanagements erfüllt hat, oder am Datenschutzaudit teilnimmt. Damit würde das Gesetz die Maßnahmen der verantwortlichen Stelle zur Verringerung des Risikos durch den Ausschluss der Gefährdungshaftung »belohnen«. Dies wäre folge-

---

72 BR-Drs. 618/88, 108.

73 S. Roßnagel/Pfitzmann/Garstka 2001, 178 ff.; für Ubiquitous Computing Möller/Bizer, in: TAUCIS 2006, 226.

74 S. Weichert, NJW 2001, 1466.

75 Wie von 1990 bis 2001 in § 8 BDSG. S. zum Vorbild des Umwelthaftungsrechts § 6 UmwHaftG.

76 S. den Regelungsvorschlag in Roßnagel/Pfitzmann/Garstka 2001, 183.

richtig: Weist nämlich die verantwortliche Stelle die Erfüllung aller technischen und organisatorischen Anforderungen für ihre Datenverarbeitung nach, geht von ihrer Datenverarbeitung keine gesteigerte Gefährdung für die informationelle Selbstbestimmung mehr aus.[77]

5.1.10 Institutionalisierte Grundrechtskontrolle

Der Schutz der informationellen Selbstbestimmung bedarf einer objektiven Ordnung, die in der Praxis mehr und mehr an die Stelle individueller Rechtewahrnehmung tritt. Zwar unterliegt jede Form der Kontrolle durch den Betroffenen wie durch externe Kontrollstellen den bereits beschriebenen Einschränkungen. Dennoch kann auf eine externe Kontrolle der Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch in der allgegenwärtigen Datenverarbeitung nicht verzichtet werden. Vielmehr muss versucht werden, die Kontrollstellen besser auszustatten und rechtlich so gut wie möglich für ihre Kontrollaufgabe zu rüsten.

Die Einhaltung von Datenschutzvorgaben kann künftig immer weniger von der individuellen Kontrolle des Betroffenen abhängig gemacht werden.[78] Sie muss in noch viel stärkerem Maß stellvertretend Kontrollverfahren und Kontrollstellen übertragen werden, die das Vertrauen der Betroffenen genießen. Dies sind zum einen die Datenschutzbeauftragten, denen weitergehende Eingriffsbefugnisse für grobe Missbrauchsfälle zuerkannt werden müssen.[79] Auch wird Verantwortung für die adäquate Technikgestaltung stärker zu institutionalisieren sein – etwa in Form von Verantwortlichen der Geschäftsleitung und der betrieblichen

[77] S. näher Roßnagel/Pfitzmann/Garstka 2001, 181.

[78] Der Vorschlag von Möller/Bizer, in: TAUCIS 2006, 226, die erhöhte Komplexität der Verarbeitung und das zusätzliche Massenproblem vor allem dadurch aufzufangen, dass »eine stärkere Selbstkontrolle der Verarbeitungen durch die Betroffenen« stattfindet, dürfte diese maßlos überfordern.

[79] S. näher Roßnagel/Pfitzmann/Garstka 2001, 194 ff.

Datenschutzbeauftragten. Schließlich werden anerkannte Datenschutzverbände eine Art Ombudsfunktion wahrnehmen und mit entsprechenden Klagebefugnissen ausgestattet sein müssen.[80]

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.

5.2 Konsequenzen für die Modernisierung des Datenschutzrechts

Der Gesetzgeber darf mögliche oder gar absehbare, die Freiheit gefährdende Entwicklungen nicht unberücksichtigt lassen. Ihn trifft eine Schutzpflicht für die Grundrechte und die demokratische Struktur unserer Gesellschaft.[81] Selbst wenn er diese zu einem bestimmten Zeitpunkt durch gesetzliche Vorkehrungen erfüllt, hat er bei einer Veränderung der Umstände und – mit ihnen – der Risiken eine Nachbesserungspflicht.[82] Um dieser rechtzeitig nachkommen zu können, trifft ihn eine Pflicht zur Beobachtung der Entwicklung.[83] Der Gesetzgeber hat »wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels, … die technischen Entwicklungen aufmerksam zu beobachten und notfalls durch ergänzende Rechtssetzung korrigierend einzugreifen«.[84]

Allgegenwärtige Datenverarbeitung macht solche Korrekturen erforderlich. Sie erschwert durch ihre Verbreitung, ihre Datenvermehrung, ihre Alltäglichkeit, ihre Unmerklichkeit, ihre Intransparenz und ihre Komplexität nicht nur den Vollzug des geltenden Datenschutzrechts. Vielmehr stellen darüber hinaus

[80] S. näher Roßnagel/Pfitzmann/Garstka 2001, 130 ff., 143 ff. und 205 ff.

[81] BVerfGE 49, 89 (140).

[82] BVerfGE 65, 1 (56).

[83] BVerfGE 112, 304 (316).

[84] BVerfGE 112, 304 (320f.), BVerfG, K&R 2007, 32 (38).

die Grundprinzipien ihrer Konzeption das gegenwärtige Schutzprogramm für das Grundrecht auf informationelle Selbstbestimmung grundsätzlich konzeptionell in Frage. Ohne Anpassung des Datenschutzrechts an die durch allgegenwärtige Datenverarbeitung bewirkten Veränderungen wird die Verwirklichung dieses Grundrechts gefährdet.

Zugleich aber wird informationelle Selbstbestimmung als normatives Konzept für die freie Entfaltung von Individuen und die demokratische Entwicklung der Gesellschaft immer wichtiger. Bedingung ihrer Verwirklichung ist jedoch ein modifiziertes und ergänztes Schutzprogramm, in dem die Konzepte und Instrumente des Datenschutzes der Allgegenwärtigkeit der Datenverarbeitung angepasst sind. 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.

Allgegenwärtige Datenverarbeitung wird nicht über Nacht Realität, sondern wird Schritt für Schritt entwickelt und eingeführt. Übertriebene Hysterie und Hektik sind daher ebenso falsch wie beruhigendes Untätigbleiben. Derzeitige RFID-Anwendungen führen nicht bereits zum Verlust jeglicher Selbstbestimmung. Aber – RFID-Chips sind nicht nur die Nachfolger des Barcodes, die genauso wenig gesetzgeberische Aufmerksamkeit benötigen wie dieser. RFID-Anwendungen, Verkehrstelematik, Handy-Kameras und Location Based Services sind alle Vorboten einer großen technikgetriebenen Umwälzung der Verhältnisse. Es wäre fahrlässig, diese Entwicklungsperspektive zu ignorieren. Wir müssen uns rechtzeitig auf die Verwirklichungsbedingungen für die informationelle Selbstbestimmung unter den Bedingungen allgegenwärtiger Datenverarbeitung einrichten und den dafür erforderlichen Rechtsrahmen bestimmen.

Allerdings können wir uns nach und nach auf die Veränderungen einstellen. Dabei dürfen aber weder die verschiedenen Techniken, noch ihre Einführungsschritte, noch die erforderliche Anpassung der Gesetze als jeweils getrennte Ereignisse gesehen werden. Vielmehr müssen sie als Teile einer zusammenhängenden Entwicklung wahrgenommen werden, die eine integrierte Strategie der Rechtsfortbildung erfordert. Aus dieser können dann einzelne gesetzliche Vorhaben im Zeitablauf abgeleitet werden.

Eine Modernisierung des Datenschutzrechts ist ohnehin überfällig. Auch diese fordert eine längerfristige Strategie, weil die Modernisierung ebenfalls in mehreren Schritten erfolgen dürfte. Beide Strategien, die zur Modernisierung und die zur Anpassung an die Bedingungen allgegenwärtiger Datenverarbeitung, sollten miteinander verbunden werden. Ein künftiges technik- und risikoadäquates Datenschutzrecht muss beiden Herausforderungen gerecht werden.

5.3 Handlungsbedarf

Allgegenwärtige Datenverarbeitung ist eine Dual Use-Technologie. Sie ermöglicht Erleichterungen und Unterstützungen durch Delegation von unerwünschten Aufgaben an Technik, kontextbezogene Assistenz, technische Sicherheitsgewährleistung und Ergänzung unserer körperlichen und geistigen Fähigkeiten. Sie ermöglicht aber auch eine umfassende Überwachung und Rekonstruktion vieler oder gar aller Ereignisse im Leben eines Menschen. Die dadurch entstehende Informationsmacht über die jeweils Betroffenen kann die bestehende Machtverteilung in der Gesellschaft stark verändern. Dass die Betroffenen vielfach andere ebenfalls kontrollieren können, stärkt ein Zusammenleben in Freiheit nicht. Ob wir aufgrund dieser Dual Use-Eigenschaft mit allgegenwärtiger Datenverarbeitung besser leben als ohne diese Technologie, ist letztlich auch eine Frage des Datenschutzes.

Die Versprechen allgegenwärtiger Datenverarbeitung werden eine große Faszination auslösen. Dennoch wird sie nur mit hoher Akzeptanz breite gesellschaftliche Wirklichkeit werden. Die Nutzer werden auch mit diesen Techniken selbstbestimmt und eigensinnig umgehen.[85] Um selbsttätig agierende Techniken in der unmittelbaren Lebensumgebung zu akzeptieren, müssen sie durch Erfahrung Vertrauen in die Nützlichkeit und störungsfreie Funktion der Systeme, in die Sicherheit vor Angriffen und vor allem in die Respektierung ihrer informationellen Selbstbestimmung gewinnen.[86]

Die Entwicklung zu einer Welt allgegenwärtiger Datenverarbeitung gefährdet jedoch grundsätzlich die informationelle Selbstbestimmung, weil sie deren gegenwärtiges Schutzprogramm weitgehend leer laufen lässt. Es wäre jedoch eine Illusion zu glauben diese Entwicklung könnte deshalb aufgehalten oder gar verboten werden. Hierfür sind die Anreize, die Versprechen der allgegenwärtigen Datenverarbeitung ernst zu nehmen, viel zu hoch. Ein solcher Versuch würde den Datenschutz jeder Akzeptanz berauben.

Dennoch darf das Ziel der informationellen Selbstbestimmung nicht aufgegeben werden. Sie ist in einer Welt allgegenwärtiger Datenverarbeitung wichtiger als je zuvor. Notwendig ist jedoch eine Modernisierung des Datenschutzrechts, die den künftigen Bedingungen allgegenwärtiger Datenverarbeitung gerecht wird. Ob mit solchen Veränderungen die informationelle Selbstbestimmung in einer Welt allgegenwärtiger Datenverarbeitung gewährleistet werden kann, muss bis zum Beweis durch die Praxis als offen gelten. Sie sind eine notwendige, aber keine hinreichende Bedingung für einen Schutz der informationellen Selbstbestimmung.

Hinzukommen muss eine Technikforschung und -entwicklung, -standardisierung und -gestaltung, die nicht nur von Anfang an

[85] S. Lantermann 2007; Stieler, c't 2004/16, 83.

[86] S. ähnlich Heesen, in: NEXUS 2005, 199.

die Folgen der Techniknutzung für die informationelle Selbstbestimmung berücksichtigt, sondern auch technische Lösungen für System- und Selbstdatenschutz findet. Sie muss aktiv nach Lösungen dafür suchen, die Erfüllung der technischen Funktionen von ihrem Potenzial zur Kontrolle zu entkoppeln und die Handlungsmacht der Betroffenen technisch zu stärken.

Hinzukommen muss weiterhin eine umfassende Aufklärung durch sachgerechte und interessenfreie Information über Möglichkeiten und Risiken allgegenwärtiger Datenverarbeitung. Diese muss vor allem auch Hinweise zu Schutz- und Handlungsmöglichkeiten des einzelnen Nutzers enthalten. Öffentliche Debatten über allgegenwärtige Datenverarbeitung finden bereits statt und sollten positiv verstärkt werden.

Hinzukommen muss schließlich bei den Individuen das Bewusstsein, dass informationelle Selbstbestimmung ein hohes, aber gefährdetes Gut ist, und der Wunsch, es zu bewahren. In der Gesellschaft muss die Erkenntnis entwickelt werden, dass hierfür Strukturänderungen erforderlich sind, und der politische Wille, sie auch umzusetzen. Ohne die dargestellten Anpassungen dürfte jedoch die Vorhersage nicht schwer sein, dass die informationelle Selbstbestimmung schleichend ihrer Bedeutungslosigkeit entgegen geht.

6. ZUSAMMENFASSUNG

Die Entwicklungen der Informations- und Kommunikationstechnik ermöglichen eine Zukunft, in der die Verarbeitung von Daten nicht mehr nur in spezifischen Computern mit Tastatur und Bildschirm stattfindet, sondern in (nahezu) allen uns umgebenden Alltagsdingen. Sie werden durch Sprache, Gestik, Mimik oder Berührung gesteuert oder erkennen aus den Umständen selbst, was von ihnen erwartet wird. Sie präsentieren die benötigten Informationen auf den Oberflächen von Wänden oder Gegenständen, in Brillen, Kleidung oder Kopfhörern. Vielfach führen sie die erforderlichen oder gewünschten Aktionen selbsttätig aus.

Diese allgegenwärtige Datenverarbeitung verspricht, Menschheitsträume zu erfüllen. Sie verspricht eine Erweiterung der menschlichen Sinne durch Sensoren und Kontexterfassung, eine Verbesserung des menschlichen Gedächtnisses durch ein »Gedächtnis« der Dinge, eine Befreiung und Erleichterung von Arbeit durch deren Delegation auf Technik sowie eine Erhöhung der Sicherheit durch technikgestützte Kontrolle aller Lebensumstände. Die Hoffnung auf die Erfüllung dieser Träume verschafft der allgegenwärtigen Datenverarbeitung eine enorme Durchsetzungskraft.

Die gleiche Technik ermöglicht aber auch die Verwirklichung von Alpträumen. Die Vielfalt der Datenverarbeitung führt zu einer exponentiellen Zunahme von personenbezogenen Daten mit hoher Aussagekraft. Sie erlauben, individuelles Verhalten ebenso detailliert nachzuvollziehen wie kollektive Lebensstrukturen. Allgegenwärtige Datenverarbeitung erfordert eine Infrastruktur zur permanenten Erhebung und situationsadäquaten Auswertung personenbezogener Daten, die eine potenziell perfekte Überwachung ermöglicht.

Welche Zukunft Wirklichkeit wird, hängt entscheidend davon ab, welche Bedeutung künftig dem Schutz der informationellen Selbstbestimmung zukommt. Er ist Aufgabe des Datenschutzrechts, die informationelle Selbstbestimmung zu gewährleisten. Dieses erscheint zwar in der Lage, Risiken zu beherrschen, soweit nur wenige Instanzen mit klarer Rollenzuweisung beteiligt sind, die Verhältnisse überschaubar sind und die zu beurteilenden Handlungen nur Einzelfälle betreffen. Allgegenwärtige Datenverarbeitung verändert jedoch weitgehend die Interaktion des Menschen mit Informationstechnik grundsätzlich und schafft dadurch Verhältnisse, in denen viele Beteiligte mit ständig wechselnden Rollen mitwirken, vielfältige Zwecke gleichzeitig verfolgt werden, Daten auch in privaten oder gemischt privatgeschäftlichen Kontexten verwendet werden, die Datenverarbeitung spontan von den Techniksystemen selbst organisiert wird, für den Betroffenen unbemerkt erfolgt und in ihren Wirkungen undurchschaubar ist.

Auf diese neuen Verhältnisse sind die Grundsätze des datenschutzrechtlichen Schutzprogramms kaum anwendbar. Die Ziele, die mit dem Einsatz allgegenwärtiger Datenverarbeitung verfolgt werden, widersprechen den Zielen, die den Prinzipien des Datenschutzrechts zugrunde liegen. Grundsätze wie Transparenz, Zweckbindung, Erforderlichkeit, Kontrollfähigkeit und Mitwirkung des Betroffenen haben kaum noch Chancen, verwirklicht zu werden. Im Konflikt dürfte entscheidend sein, dass die Anwendungen allgegenwärtiger Datenverarbeitung den Betroffenen in den meisten Fällen nicht aufgedrängt, sondern von diesen gewollt werden.

Dennoch darf das Ziel der informationellen Selbstbestimmung nicht aufgegeben werden. Sie ist in einer Welt allgegenwärtiger Datenverarbeitung wichtiger als je zuvor. Notwendig ist jedoch eine Modernisierung des Datenschutzrechts, die den künftigen Bedingungen allgegenwärtiger Datenverarbeitung gerecht wird. Erforderlich ist es vor allem, Datenschutz in die Technik zu integrieren und deshalb auch Anforderungen an Technikentwickler

und -gestalter zu formulieren. Für sie müssen Anreize geschaffen werden, Datenschutzschutz von Anfang an zu berücksichtigen. Notwendig sind freiheitsförderliche Architekturen der Informations- und Kommunikationstechnik, die verhindern, dass allgegenwärtige Datenverarbeitung zu allgegenwärtiger Kontrolle wird.

LITERATURVERZEICHNIS

Abel, R.-B. (2003): Behördliche Datenschutzbeauftragte, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 890–912.

acatech (2006): RFID wird erwachsen – Deutschland sollte die Potenziale der elektronischen Identifikation nutzen, Stuttgart.

Ahrend, V./Bijok, B.-C./Dieckmann, U./Eitschberger, B./Eul, H./Guthmann, M./Schmidt, M./Schwarzhaupt, P.-D. (2003): Modernisierung des Datenschutzes?, Datenschutz und Datensicherheit (DuD) 27 (7), 433–438.

AK Technik (2006): Arbeitskreis »Technische und organisatorische Datenschutzfragen« der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe »Datenschutzgerechter Einsatz von RFID« vom 14.12.2006.

Artikel-29-Datenschutzgruppe (2005a): Arbeitsdokument 105 »Datenschutzfragen im Zusammenhang mit der RFID-Technik«, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf.

Artikel-29-Datenschutzgruppe (2005b): Arbeitsdokument 111 »Ergebnisse der öffentlichen Konsultation über Arbeitspapier 105 der Artikel-29-Datenschutzgruppe zu Datenschutzfragen im Zusammenhang mit der RFID-Technik«, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_de.pdf.

André, E./Rist, T. (2001): Controlling the Behavior of Animated Presentation Agents in the Interface: Scripting versus Instructing. AI-Magazine, Vol. 22, Nr. 4.

Bär, W. (2007): Anmerkung zum Beschluss des Ermittlungsrichters beim BHG vom 25.11.2006, Multimedia und Recht (MMR) 10 (3), 175–177.

Bartels, O./Ahlers, E. (2004): Gegenspionage – RFID-Detektor im Taschenformat, c't 9/2004, 132–136.

Bäumler, H. (1999): Das TDDSG aus Sicht eines Datenschutzbeauftragten, Datenschutz und Datensicherheit (DuD) 23 (5), 258–262.

Bäumler, H. (2002): Marktwirtschaftlicher Datenschutz, Datenschutz und Datensicherheit (DuD) 26 (6), 325–329.

Bäumler, H. (2004): Ein Gütesiegel auf den Datenschutz, Datenschutz und Datensicherheit (DuD) 28 (2), 80 – 84.

Bäumler, H./v. Mutius, A. (2002): Datenschutz als Wettbewerbsvorteil, Braunschweig.

Bergmann, L./Möhrle, R./Herb, A. (1995): Datenschutzrecht: Handkommentar, 4 Bände, (Loseblattsammlung) Stuttgart 1995 ff.

Bizer, J. (2004): Strukturplan modernes Datenschutzrecht, Datenschutz und Datensicherheit (DuD), 28 (1), 6 – 14.

Bizer, J. (2006): Bausteine eines Datenschutzaudits, Datenschutz und Datensicherheit (DuD) 30 (1), 5 – 12.

BMBF (Bundesministerium für Bildung und Forschung) (2007): IKT 2020 – Forschung für Innovationen, Berlin.

Bohn, J./Coroama, V./Langheinrich, M./Mattern, F./Rohs, M. (2002): Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge, www.inf.ethz.ch/vs/publ/papers/allvercom.pdf.

Brandl, H. (2005): Trusted Computing – Aktuelle Anwendungen, Datenschutz und Datensicherheit (DuD), 29 (9), 537–541.

BSI (Bundesamt für die Sicherheit in der Informationstechnik) (2003): Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, Ingelheim.

BSI (Bundesamt für die Sicherheit in der Informationstechnik) (2004): Risiken und Chancen des Einsatzes von RFID-Systemen, Ingelheim.

BSI (Bundesamt für die Sicherheit in der Informationstechnik) (2006): Pervasive Computing – Entwicklungen und Auswirkungen, Ingelheim.

Busch, C./Pinsdorf, U. (2007): Mobile Agenten im elektronischen Geschäftsverkehr, in: Gitter, R./Lotz, V./Pinsdorf, U./Roßnagel, A. (Hrsg.) (2007): Sicherheit und Rechtsverbindlichkeit mobiler Agenten, Wiesbaden, 9–20.

Cavazza, M. et al. (2004): Multimedial acting in mixed reality interactive storytelling, EEEE Multimedia, 11 (3), 30–39.

Cas, J. (2002): Privacy in Ubiquitous Computing Environments?, in: Proceedings 13th IST-Europe Regional Conference, Madrid, Spain, September 8–10, 2002.

COBIS (o.J.): Collaborative Business Items, http://www.cobis-online.de/.

Conrad, I. (2005): RFID-Ticketing aus datenschutzrechtlicher Sicht, Computer und Recht (CR) 21 (7), 537–544.

Cornelius, K. (2002): Vertragsabschluss durch autonome elektronische Agenten, Multimedia und Recht (MMR) 5 (6), 353–358.

Coroama, V. (2006): Pervasive Computing im Alltag, digma 3/2006, 106–109.

Coroama, V./Langheinrich, M. (2005): The Smart Tachograph, http://www.vs.inf.ethz.ch/publ/papers/ubicomp2005-tachograph-video.pdf.

Coroama, V./Langheinrich, M. (2006): Personalized Vehicle Insurance Rates – A Case for Client-Side Personalization in Ubiquitous Computing in: Proceedings Workshop on Privacy-Enhanced Personalization at CHI, Montreal, Canada, April 22.

Coroama, V. u.a. (2003): Szenarien des Kollegs Leben in einer smarten Umgebung – Auswirkungen des Ubiquitous Computing, Ladenburg.

Crutzen, C. K. M. (2005): Intelligent Ambience Between Heaven and Hell, Journal of Information, Communication and Ethics in Society (ICES), 3 (4), Paper 7.

Dammann, U./Simitis, S. (1997): Europäische Datenschutzrichtlinie – Kommentar, Baden-Baden.

Dierstein, R. (2004): Sicherheit in der Informationstechnik – der Begriff der IT-Sicherheit. Informatik-Spektrum 27 (4), 343–353.

Dix, A. (2003): Konzepte des Systemdatenschutzes, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 363–386.

Eberspächer, J./v. Reden, W. (Hrsg.) (2006): Umhegt oder abhängig. Der Mensch in einer digitalen Umgebung, Berlin, Heidelberg.

Eckert, C.: Mobil, aber sicher, in: Mattern, F. (Hrsg.), Total vernetzt, Berlin, 91 – 122.

Eckert, C./Bayarou, K./Rohr, S. (2004): NGN, All-IP, B3G: Enabler für das Future-Net, Überblick über Entwicklungen im Bereich zukünftiger Netze, Informatik-Spektrum 27 (1), 12–34.

Ehmann, H. (1988): Zur Zweckbindung privater Datennutzung, Recht der Datenverarbeitung (RDV) 4 (4), 169–180; 4 (5), 221–247.

Eisenberg, U./Puschke, J./Singelnstein, T. (2005): Überwachung mittels RFID-Technologie, Zeitschrift für Rechtspolitik (ZRP) 38 (1), 9–12.

Ernst, S. (2005): Rechtliche Probleme mobiler Ad-Hoc-Netze, in: Taeger, J./Wiebe, A. (Hrsg.), Mobilität – Telematik – Recht, Köln, 127–144.

Europäische Kommission: Ambient Assisted Living (AAL) for the Ageing Society, http//www.cordis.lu/ist/so/aal/home.html.

Fabian, B./Günter, O./Spiekermann, S. (2005): Security analysis of the object name service for RFID, in: Proceedings of the 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing.

FifF (2006): Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (Hrsg.), RFID – Radio Frequency Identification, Bremen.

Finkenzeller, K. (2002): RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Aufl. München.

Fishkin, K. P./Roy, S. (2003): Enhancing RFID Privacy via Antenna Energy Analysis, Proc. of MIT RFID Privacy Workshop, Boston, November.

Fleisch, E./Christ, O./Dierkes, M. (2005): Die betriebswirtschaftliche Vision des Internets der Dinge, in: Fleisch, E./Mattern, F. (Hrsg.) (2005): Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg, 3–38.

Fleisch, E./Dierkes, M. (2003): Betriebswirtschaftliche Anwendungen des Ubiquitous Computing – Beispiele, Auswirkungen und Visionen, in: Mattern, F. (Hrsg.), Total vernetzt, Berlin, Heidelberg, 143–158.

Fleisch, E./Mattern, F. (Hrsg.) (2005): Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg.

Flörkemeier, C. (2005): EPC-Technologie – vom Auto-ID Center zu EPCglobal, in: Fleisch, E./Mattern, F. (Hrsg.) (2005): Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg, 87–100.

Flörkemeier C./Schneider, R./Langheinrich, M. (2004): Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf.

Garstka, H. (2006): Lokationsdaten – auf dem Weg zur Rundumüberwachung, 44. Deutscher Verkehrsgerichtstag 2006, Hamburg, 125–131.

Garstka, H./Gill, D. (2003): Datenschutzbeauftragte der Länder, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 787–802.

Gitter, R. (2007): Softwareagenten im elektronischen Geschäftsverkehr – Rechtliche Vorgaben und Gestaltungsvorschläge, Baden-Baden.

Gitter, R./Roßnagel, A. (2003): Rechtsfragen mobiler Agentensysteme im E-Commerce. Kommunikation und Recht (K&R) 2003, 64–72.

Gitter, R./Lotz, V./Pinsdorf, U./Roßnagel, A. (Hrsg.) (2007): Sicherheit und Rechtsverbindlichkeit mobiler Agenten, Wiesbaden.

Gola, P./Schomerus, R. (2006): Bundesdatenschutzgesetz-Kommentar, 8. Aufl., München.

Gupta, P./Hoffmann, M./Holtkamp, B./Möhr, W./Peters, J./Ritscher, M./Voisard, A. (2004): Mobile kontextabhängige Multimediadienste, Informatik-Spektrum 27 (1), 35–43.

Hansen, M./Krasemann, H./Rost, M./Genghini, R. (2003): Datenschutzaspekte von Identitätsmanagementsystemen, Datenschutz und Datensicherheit (DuD) 27 (9), 551–555.

Hansen, M./Wiese, M. (2004): Gateway, RFID – Radio Frequency Identification, Datenschutz und Datensicherheit (DuD) 28 (3), 109.

Heil, H. (2003): Bundesbeauftragter für den Datenschutz, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 748–786.

Herrtwich, R. G. (2003): Fahrzeuge am Netz, in: Mattern, F. (Hrsg.), Total vernetzt, Szenarien einer informatisierten Welt, Berlin, Heidelberg, 63–84.

Herrtwich, R. G./Rehborn, H./Franz, W./Wex, P. (2006): Lokationsdaten – auf dem Weg zur Rundumüberwachung, 44. Deutscher Verkehrsgerichtstag 2006, Hamburg, 132–141.

Hillenbrand-Beck, R. (2003): Aufsichtsbehörden, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 817–448.

Hoffmann-Riem, W. (1997): Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer, L./Micklitz, H.-W./Tonner, K. (Hrsg.), Recht und diffuse Interessen in der Europäischen Rechtsordnung, Baden-Baden, 777–788.

Hoffmann-Riem, W. (1998): Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes –, Archiv des öffentlichen Rechts (AöR) 123 (4), 1998, 514–540.

Holznagel, B./Bonnekoh, M. (2006): RFID – Rechtliche Dimensionen der Radiofrequenz-Identifikation, Berlin.

Holznagel, B./Bonnekoh, M. (2006): Radio Frequency Identification – Innovation vs. Datenschutz?, Multimedia und Recht (MMR) 9 (1), 17–23.

Holznagel, B./Sonntag, M. (2003): Einwilligung des Betroffenen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 680–715.

Hornung, G. (2004): Zwei runde Geburtstage: das Recht auf informationelle Selbstbestimmung und das WWW, Multimedia und Recht (MMR) 7 (1), 3–8.

Hornung, G. (2006): RFID und datenschutzrechtliche Transparenz, Multimedia und Recht (MMR) 9 (5), XX–XXII.

Hornung, G. (2007): Ermächtigungsgrundlage für den »Bundes-Trojaner«? Verfassungsrechtliche Anforderungen und Grenzen für die so genannte Online-Durchsuchung im Ermittlungsverfahren, i.E.

Hubig, C. (2003): Selbständige Nutzer oder verselbständigte Medien – Die neue Qualität der Vernetzung, in: Mattern, F. (Hrsg.), Total vernetzt, 211–230.

Hubig, C. (2007): Der technisch aufgerüstete Mensch – Auswirkungen auf unser Menschenbild, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 152–162.

Huber, A. (2006): Radiofrequenz-Identifikation. Die aktuelle Diskussion in Europa, Multimedia und Recht (MMR) 9 (11), 728–734.

Internationale Konferenz der Datenschutzbeauftragten: Entschließung zu Radio-Frequency Identification vom 20.11.2003, http://www.privacyconference2003.org/resolutions/RFIDResolutionGE.doc.

ISTAG (2001): The Information Society Technology Advisory Group (Ducatel, K, Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J-C.), Scenarios for Ambient Intelligence 2010 – Final Report, Sevilla, http://www.hltcentral.org/usr_docs/ISTAG-Final.pdf.; http://www.cordis.lu/ist/istag.htm.

Jahn, M./Kudlich, H. (2007): Die strafprozessuale Zulässigkeit der Online-Durchsuchung, Juristische Rundschau (JR) 83 (2), 57–61.

Jandt, S. (2007): Datenschutz bei Location Based Services, Multimedia und Recht (MMR) 10 (2), 74–78.

Jandt, S./Laue, P. (2006): Voraussetzungen und Grenzen der Profilbildung bei Location Based Services, Kommunikation und Recht (K&R) 2006, 316–320.

Juels, A. (2004): Minimalist cryptography for low-cost RFID tags. The Fourth International Conference on Security in Communication Networks (SCN 2004), Berlin u.a.

Juels, A./Syverson, P./Bailey, D. (2005): High-power proxies for enhancing RFID privacy and utility. Workshop on Privacy Enhancing Technologies (PET 2005).

Juels, A./Rivest, R. L./Szydlo, M. (2003): The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, in: Atluri (Ed.), Proc. of the 8th ACM Conference on Computer and Communications Security, 103–111.

Kelter, H./Wittmann, S. (2004): Radio Frequency Identification – RFID, Datenschutz und Datensicherheit 28 (6), 331–334.

Kilian, W. (2002): Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? Zum Modernisierungsgutachten 2002 für den Bundesminister des Innern, in: Bizer, J./Lutterbeck, B./Rieß, J. (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, Berlin 2002, 151–160.

Köhntopp, M. (2001): Datenschutz und »Privacy Enhancing Technologies«, in: Roßnagel, A. (Hrsg.), Allianz von Medienrecht und Informationstechnik?, Baden-Baden, 55–66.

Königshofen, T. (2003): Betriebliche Datenschutzbeauftragte, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 852–889.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2006): Entschließung vom 26./27.10.2006: Verbindliche Regelungen für den Einsatz von RFID-Systemen, abgedruckt in: Der Hessische Datenschutzbeauftragte, 35. Tätigkeitsbericht, Wiesbaden, 193–194.

Kugler, D. (2005): Risiko Reisepass, c't 2005 (5), 84–89.

Kügler, D./Naumann, I. (2007): Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass – Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen, Datenschutz und Datensicherheit (DuD) 31 (3), 176–180.

Kuhnhenn, K./Urban, A. I./Morgan, R. M. (2006): Von individueller Produktverantwortung bis zu erhöhter Anlagenkontrolle – verbessertes WEEE-Recycling durch RFID-Anwendungen, in: Urban, A./Halm, G./Morgan, R. M. (Hrsg.), Stoffströme der Kreislaufwirtschaft, Kassel, 85–94.

Kunig, P. (1993): Der Grundsatz informationeller Selbstbestimmung, Jura 15 (12), 595–603.

Lahner, C. M. (2004): Anwendung des § 6c BDSG auf RFID, Datenschutz und Datensicherheit (DuD) 28 (12), 723–726.

Lampe, M./Flörkemeier, C./Haller, S.: Einführung in die RFID-Technologie, in: Fleisch, E./Mattern, F. (Hrsg.), Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg, 69–86.

Langheinrich, M. (2001): Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, in: Abowd et al. (Eds.), Proceedings of Ubicomp 2001, 273–291.

Langheinrich, M. (2005a): Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, in: Fleisch, E./Mattern,

F. (Hrsg.): Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg, 329–362.

Langheinrich, M. (2005b): Personal Privacy in Ubiquitous Computing – Tools and System Support, Dissertation ETH Zürich.

Langheinrich, M. (2006): RFID and Privacy, in: Petkovic, M./Jonker W. (Hrsg.), Security, Privacy, and Trust in Modern Data Management, Berlin.

Langheinrich, M. (2007a): RFID und die Zukunft der Privatsphäre, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 43–69.

Langheinrich, M. (2007b): Gibt es in einer total informatisierten Welt noch eine Privatsphäre?, in: Mattern, F. (Hrsg.): Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin, i.E.

Lantermann, E.-D. (2007): Gesellschaftliche Antworten auf eine allgegenwärtige Datenverarbeitung aus einer psychologischen Perspektive, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 172–181.

Lindemann, C./Waldhorst, O. P. (2006): Peer-to-Peer-Systeme für drahtlose Multihop-Netze, Informatik-Spektrum 29 (3), 222–226.

Mattern, F. (2001a): Ubiquitous Computing, in: Kubicek H./Klumpp D./Fuchs, G./Roßnagel, A. (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg, 52–61.

Mattern, F. (2001b): Pervasive/Ubiquitous Computing, Informatik-Spektrum 24 (3), 145–147.

Mattern, F. (2002): Vom Handy zum allgegenwärtigen Computer – Ubiquitous Computing: Szenarien einer informatisierten Welt, Analysen der Friedrich Eber-Stiftung zur Informationsgesellschaft Nr. 6/2002, Berlin.

Mattern, F. (Hrsg.) (2003b): Total vernetzt, Szenarien einer informatisierten Welt, Berlin, Heidelberg.

Mattern, F. (2003c): Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing, in: ders. (Hrsg.), Total vernetzt, Berlin, Heidelberg, 1–42.

Mattern, F. (2004): Allgegenwärtige Informationstechnik – Soziale Folgen und Konsequenzen für die Menschenrechte, in: Kirchschläger, P./Kirchschläger, P./Belliger, A./Krieger, D. (Hrsg.), Menschenrechte und Terrorismus, Bern, 315–335.

Mattern, F. (2005a): Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen, in: Taeger, J./Wiebe, A. (Hrsg.), Mobilität – Telematik – Recht, Köln, 1–34.

Mattern, F. (2005b): Die technische Basis für das Internet der Dinge, in: Fleisch, E./Mattern, F. (Hrsg.), Das Internet der Dinge, Berlin u.a., 39–66.

Mattern, F. (2005c): Ubiquitous Computing – Szenarien einer informatisierten Welt, in: Zerdick, A./Picot, A../Schrape K./Burgelman, J. C./Silverstone R. (Hrsg), E-Merging Media – Digitalisierung der Medienwirtschaft, Berlin, Heidelberg, 145–163.

Mattern, F. (2007a): Allgegenwärtige Datenverarbeitung – Technologietrends und Auswirkungen, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – wie möchten wir in Zukunft leben?, 11–38, i.E.

Mattern, F. (2007b): Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing, in: ders. (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin, i.E.

Mattern, F./Langheinrich, M. (2001): Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge, in: Müller, G./Reichenbach, M. (Hrsg.) Sicherheitskonzepte für das Internet, Berlin, Heidelberg, 7–26.

Maurer, H. (2004): Der PC in zehn Jahren, Informatik-Spektrum 27 (1), 44–50.

Möller, J. (2006): Automatisiertes Management von Datenschutzrechten, Datenschutz und Datensicherheit (DuD) 30 (2), 98–101.

Moore, G. (1965): Cramming more components onto integrated circuits, Electronics, 114–117.

Morgan, R. M./Urban, A. I./Kuhnhenn, K. (2006): Entwicklungsanforderungen an RFID beim Einsatz für ein intelligentes Recycling, in: Urban, A./Halm, G./Morgan, R. M. (Hrsg.), Stoffströme der Kreislaufwirtschaft, Kassel, 123–135.

Müller, J. (2004): Ist das Auslesen von RFID-Tags zulässig?, Datenschutz und Datensicherheit (DuD) 28 (5), 215–217.

Müller, J. (2007): Datenschutzvorsorge gegenüber Risiken der RFID-Technologie, in: Mattern, F. (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin, i.E.

Müller, J./Handy, M. (2004): RFID und Datenschutzrecht, Risiken, Schutzbedarf und Gestaltungsideen, Datenschutz und Datensicherheit (DuD) 28 (11), 655–659.

Müller, J./Handy, M. (2005): RFID als Technik des Ubiquitous Computing – Eine Gefahr für die Privatsphäre, in: Ferstl, O./Sinz, E./Eckert, S./Isselhorst, T. (Hrsg.), Wirtschaftsinformatik 2005, Heidelberg, 1145–1164.

Nedden, B. (2001): Datenschutz und »Privacy Enhancing Technologies«, in: Roßnagel, A. (Hrsg.), Allianz von Medienrecht und Informationstechnik?, Baden-Baden, 67–75.

Network on Wheels (2005): DaimlerChrysler/TU München, Projekthomepage, www.network-on-wheels.de.

NEXUS (2005): Heesen, J./Hubig, C./Siemoneit, O./Wiegerling, K. (Hrsg.), Leben in einer vernetzten und informatisierten Welt – Context-Awareness im Schnittfeld von Mobile und Ubiquitous Computing, Szenarien des Sonderforschungsbereichs 627 »Umgebungsmodelle für mobile kontextbezogene Systeme«, Stuttgart.

Peters, J./Pinsdorf, U./Roth, V. (2007): Sicherheitsaspekte mobiler Agenten, in: Gitter, R./Lotz, V./Pinsdorf, U./Roßnagel, A. (Hrsg.) (2007): Sicherheit und Rechtsverbindlichkeit mobiler Agenten, Wiesbaden, 21–39.

Pfaff, D./Skiera, B. (2002): Ubiquitous Computing – Abgrenzung, Merkmale und Auswirkungen aus betriebswirtschaftlicher Sicht, in: Britzelmaier, B./Geberl, S./Weinmann, S. (Hrsg.), Wirtschaftsinformatik: Der Mensch im Netz – Ubiquitous Computing, Stuttgart, 24–37.

Raabe, F. (2006): Der Auskunftsanspruch nach dem Referentenentwurf zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, Zeitschrift für Urheber- und Medienrecht (ZUM) 38 (6), 439–443.

Rand Corporation (2005): Eine neue Zeit. Deutschland und die Informations- und Kommunikationstechnologie im Jahr 2015, Bonn.

Reimer, H. (2006): TeleTrusT: Anwendung einer vertrauenswürdigen Trusted-Computing-Technologie, Datenschutz und Datensicherheit (DuD) 30, 666.

Roßnagel, A. (1993): Rechtswissenschaftliche Technikfolgenforschung – Umrisse einer Forschungsdisziplin, Baden-Baden.

Roßnagel, A. (1997): Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer »civil information society«, Zeitschrift für Rechtspolitik (ZRP) 30 (1), 26–30.

Roßnagel, A. (Hrsg.) (1999): Recht der Multimediadienste, Kommentar zum Informations- und Kommunikationsdienstegesetz und Mediendienste-Staatsvertrag, München, Loseblatt 1999 ff.

Roßnagel, A. (2000): Datenschutzaudit – Konzeption, Durchführung, gesetzliche Regelung, Braunschweig.

Roßnagel, A. (2001): Allianz von Medienrecht und Informationstechnik: Hoffnungen und Herausforderungen, in: ders. (Hrsg.), Allianz von Medienrecht und Informationstechnik?, Baden-Baden, 17–35.

Roßnagel, A. (2002a): Freiheit im Cyberspace, Informatik-Spektrum 25 (1), 33–38.

Roßnagel, A. (2002b): Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive, in: Bizer, J./Lutterbeck, B./Rieß, J. (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, Festschrift für Büllesbach, Stuttgart, 131–142.

Roßnagel, A. (Hrsg.) (2003a): Handbuch Datenschutzrecht, München.

Roßnagel, A. (2003b): Datenschutz in Tele- und Mediendiensten, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 1280–1325.

Roßnagel, A. (2003c): Konzepte des Selbstdatenschutzes, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 325–352.

Roßnagel, A. (2003d): Datenschutzaudit, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 437–483.

Roßnagel, A. (Hrsg.) (2003e): Sicherheit für Freiheit? Riskante Sicherheit oder riskante Freiheit in der Informationsgesellschaft, Baden-Baden.

Roßnagel, A. (2004): Datenschutz 2015 – in einer Welt des Ubiquitous Computing, in: Bizer, J./v. Mutius, A./Petri, T. B./Weichert, T. (Hrsg.), Innovativer Datenschutz – Wünsche, Wege, Wirklichkeit, Festschrift für H. Bäumler, Kiel, 335–351.

Roßnagel, A. (2005): Modernisierung des Datenschutzrechts in einer Welt allgegenwärtiger Datenverarbeitung, Multimedia und Recht (MMR) 8 (2), 71–75.

Roßnagel, A. (2005): Verantwortung für Datenschutz, Informatik-Spektrum 28 (6), 462–473.

Roßnagel, A. (2005): Das rechtliche Konzept der Selbstbestimmung in der mobilen Gesellschaft, in: Taeger, J./Wiebe, A. (Hrsg.), Mobilität – Telematik – Recht, Köln, 53–75.

Roßnagel, A. (2006): Vorratsspeicherung von Verkehrsdaten in Europa, Zeitschrift für Europarecht (EuZ) 8 (2), 30–35.

Roßnagel, A. (2006): Datenschutz in der künftigen Verkehrstelematik, Neue Zeitschrift für Verkehrsrecht (NVZ) 19 (6), 281–288.

Roßnagel, A. (2006): Datenschutz bei der künftigen Kommunikation vom und zum Kraftfahrzeug, in: Deutsche Akademie für Verkehrswissenschaft (Hrsg.), 44. Deutscher Verkehrsgerichtstag 2006, Hamburg, 142–161.

Roßnagel, A. (2007): Personalisierung in der E-Welt – Aus dem Blickwinkel der informationellen Selbstbestimmung gesehen, Wirtschaftsinformatik (WI), 49 (1), 8–15.

Roßnagel, A. (2007): Datenschutz in der Welt allgegenwärtigen Rechnens, Informationstechnik (it) 49 (2), 83–90.

Roßnagel, A. (2007): Selbst- oder Fremdbestimmung – die Zukunft des Datenschutzes, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 126–151.

Roßnagel, A. (2007): Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing, in: Mattern, F. (Hrsg.): Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin, i.E.

Roßnagel, A./Banzhaf, J./Grimm, R. (2003): Datenschutz im Electronic Commerce, Heidelberg.

Roßnagel, A./Jandt, S./Müller, J./Gutscher, A./Heesen, J. (2006): Datenschutzfragen mobiler kontextbezogener Systeme, Wiesbaden.

Roßnagel, A./Müller, J. (2004): Ubiquitous Computing – Neue Herausforderungen für den Datenschutz, Computer und Recht 20 (8), 625–632.

Roßnagel, A./Pfitzmann, A/Garstka, H. (2001): Modernisierung des Datenschutzrechts. Bundesministerium des Inneren, Berlin.

Roßnagel, A./Schnellenbach-Held, M./Geibig, O./Paul, S. (2007): Rechtssichere agentenbasierte Vergabeverfahren – Am Beispiel von Vergabeverfahren für Bauleistungen, Baden-Baden.

Roßnagel, A./Scholz, P. (2000): Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, Multimedia und Recht (MMR) 3 (12), 721–729.

Roßnagel, A./Schroeder, U. (1999): Multimedia in immissionsschutzrechtlichen Genehmigungsverfahren, Köln.

Roßnagel, A./Sommerlatte, T./Winand, U. (2007): Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E.

Rothermel, K. (2007): Kontextbezogene Systeme – Die Welt im Computer modelliert, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 31–42.

Rothermel, K./Bauer, M./Becker, C. (2003): Digitale Weltmodelle – Grundlage kontextbezogener Systeme, in: Mattern, F. (Hrsg.), Total vernetzt, Berlin u.a., 134–142.

Samuelson, P. (2000): Privacy as Intellectual Property? In: Stanford Law Review 52 (2000), 1125–1167.

Sarma, S. E./Weis, S.A./Engels, D. W. (2002): RFID Systems and Security and Privacy Implications, in: Kaliski, B./Co, C. K./Paar, C. (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2002, 454–469.

Satyanarayanan, M. (2001): M. Satyanarayanan on Mobile and Pervasive Computing (Interview), IEEE Distributed Systems Online, 2 (6), 2001.

Schaar, P. (2002): Datenschutz im Internet, München 2002.

Schaffland, H.-J./Wiltfang, N. (1991): Bundesdatenschutzgesetz: Kommentar nebst einschlägigen Rechtsvorschriften, Loseblattsammlung, Berlin 1991 ff.

Schläger, U. (2004): Gütesiegel nach Datenschutzauditverordnung Schleswig-Holstein, Datenschutz und Datensicherheit (DuD) 28 (8), 459–461.

Schmid, V. (2005): Mastering the Legal Challenges, in: Heinrich, C. (Ed.), RFID and Beyond, Indianapolis, 193–207.

Scholz, P. (2003): Datenschutz bei Data Warehousing und Data Mining, in: Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht, München, 1833–1875.

Scholz, P. (2003): Datenschutz beim elektronischen Einkaufen und Bezahlen, Baden-Baden.

Schulz, W. (1999): Verfassungsrechtlicher »Datenschutzauftrag« in der Informationsgesellschaft, Die Verwaltung 32 (2), 137–177.

Schwenke, M. (2006): Datenschutz und Individualisierung – Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Eigen- und Fremdindividualisierung, Wiesbaden.

Sietmann, R. (2004): Die Instrumentierung der Lebenswelt – Gesellschaftliche Auswirkungen des Pervasive Computing, c't 2004/16, 84–90.

Simitis, S. (1984): Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, Neue Juristische Wochenschrift (NJW) 37 (8), 398–405.

Simitis, S. (2000): Auf dem Weg zu einem neuen Datenschutzkonzept, Datenschutz und Datensicherheit (DuD) 24 (12), 714–726.

Simitis, S. (Hrsg.) (2006): Bundesdatenschutzgesetz-Kommentar, 6. Aufl. Baden-Baden.

Skiera, B./Spann. M. (2002): Preisdifferenzierung im Internet, in: Schlögel, M./Tomczak, T./Belz, C. (Hrsg.), Roadm@p to E-Business – Wie Unternehmen das Internet erfolgreich nutzen, St Gallen, 270–284.

Solove, D. J. (2006): A Taxonomy of Privacy. In: University of Pennsylvania Law Review, Vol. 154, No 3 (2006), 477–560.

Sommerlatte, T. (2007): Technikgestaltung aus Sicht des Nutzers, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 164–170.

Staudinger, J. v. (1999): Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Zweites Buch. Recht der Schuldverhältnisse. §§ 823–825, 13. Bearbeitung, Berlin.

Stechow, C. v. (2005): Datenschutz durch Technik – Rechtliche Förderungsmöglichkeiten datenschutzfördernder Technik am Beispiel der Videoüberwachung und des Privacy Filters, Wiesbaden.

Steinmetz, R./Wehrle, K. (2004): Peer-to-Peer-Networking & -Computing, Informatik-Spektrum 27 (1), 51–54.

Steinmüller, W. (1993): Informationstechnologie und Gesellschaft, Darmstadt.

Stieler, W. (2004): Smarte Begleitung – Pervasive computing durchdringt den Alltag, c't 2004/16, 78–83.

Stumpf, F./Sacher, M./Roßnagel, A./Eckert, C. (2007): Erzeugung elektronischer Signaturen mittels Trusted Platform Module, Datenschutz und Datensicherheit (DuD) 31 (4), 357–361.

SWAMI (2006a): Friedewald, M./Vildjiounaite, E./Wright, D. (Eds.), Safeguards in a World of Ambient Intelligence – The brave new world of ambient intelligence: A state-of-the-art review, http://swami.jrc.es/pages/documents/SWAMI_D1_Final.pdf.

SWAMI (2006b): Punie, Y./Delaitre, S./Maghiros, I./Wright, D. (Eds.): Safeguards in a World of Ambient Intelligence – Dark Scenarios in Ambient Intelligence: Highlighting risks and vulnerabilities, http://swami.jrc.es/pages/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf.

SWAMI (2006c): Friedewald, M./Lindner, R./Wright, D., Safeguards in World of Ambient Intelligence: Policy Options to Counteract Threats and Vulnerabilities – First Results, Brussels 2006.

TAUCIS (2006): Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin, Technikfolgenabschätzung Ubiquitäres Computing und informationelle Selbstbestimmung, Berlin.

Tauss, J./Kollbeck, J./Fazlic, N. (2004): Modernisierung des Datenschutzes, Wege aus der Sackgasse, in: Bizer, J./v. Mutius, A./Petri, T. B./Weichert, T. (Hrsg.), Innovativer Datenschutz – Wünsche, Wege, Wirklichkeit, Festschrift für Bäumler, Kiel, 41–52.

TA Swiss (2003): Hilty, L./Behrendt, S. u.a., Das Vorsorgeprinzip in der Informationsgesellschaft – Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt, Bern.

Thiesse, F. (2005): Architektur und Integration von RFID-Systemen, in: Fleisch, E./Mattern, F. (Hrsg.): Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg, 101–118.

Thiesse, F. (2005): Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung, in: Fleisch, E./Mattern, F. (Hrsg.), Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, Berlin, Heidelberg, 363–378.

Toutziaraki, T. (2007): Ein winzig kleiner Chip, eine riesengroße Herausforderung für den Datenschutz, Eine datenschutzrechtliche Beurteilung des Einsatzes der RFID-Technologie unter Aspekten des Europäischen Rechts, Datenschutz und Datensicherheit (DuD) 31 (2), 107–112.

Tränkler, H.-R./Schneider, F. (2001): Das intelligente Haus, München.

Trusted Computing Group (2006): Trusted Platform Module (TPM) Specifications, Technical Report, https://www.trustedcomputinggroup.org/.

Trute, H.-H. (2003): Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 156–187.

UNESCO (2007): Ethical Implications of Emerging Technologies: A Survey, prepared by Rundle, M./Conley, C., Paris.

Urban, A. I./Morgan, R. M./Kuhnhenn, K. (2006): Abfallerkennung durch Radio Frequency Identification, in: Urban, A./Halm, G./Morgan, R. M. (Hrsg.), Stoffströme der Kreislaufwirtschaft, Kassel, 85–94.

Van de Voort, M./Ligtvoet, A. (2006): Towards an RFID Policy for Europe, Brussels.

Vorwerk (2005): Erster Teppichboden mit integrierter RFID-Technologie, Pressemitteilung vom 7.6.2005, http://www.vorwerk-teppich.de/_66C58C58EEC0E6EAA1F8D077EAF3347D/rfid.html.

Warren, S./Brandeis, L. (1890): The Right to Privacy. In: Harvard Law Review 4 (1890), 193–220.

Weber, H. (2004): Future Net: Spekulationen über das Internet der Zukunft, Informatik-Spektrum 27 (1), 3–11.

Wedde, P. (2003): Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 526–545.

Wedde, P. (2003): Rechte der Betroffenen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München, 546–569.

Weichert, T. (1998): Datenschutzberatung – Hilfe zur Selbsthilfe, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Braunschweig, 213–229.

Weichert, T. (2001): Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, Neue Juristische Wochenschrift (NJW) 54 (20), 1463–1467.

Weiser, M. (1991): The Computer for the 21st Century, Scientific American 265 (3), 66–75.

Westerholt, M v./Döring, W. (2004): Datenschutzrechtliche Aspekte der Radio Frequency Identification, Computer und Recht (CR) 20 (9), 710–716.

Winand, U./Frankfurt, A. (2007): Neue Geschäftsfelder, wirtschaftliche Impulse und Risiken, in: Roßnagel, A./Sommerlatte, T./Winand, U. (Hrsg.), Allgegenwärtige Datenverarbeitung – Wie möchten wir in Zukunft leben?, i.E., 73–93.

Yamada, S./Kamioka, E. (2005): Access Control for Security and Privacy in Ubiquitous Computing Environment, IEICE Transactions on Communication 3/2005, 846–856.

Zezschwitz, F. v. (2003): Das Konzept der normativen Zweckbegrenzung, in: Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht, München, 219–268.

ZUM AUTOR

Alexander Roßnagel,

Dr. jur., ist Vizepräsident der Universität Kassel und Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel. Er ist zugleich wissenschaftlicher Leiter der »Projektgruppe verfassungsverträgliche Technikgestaltung (provet)« im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel sowie Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) in Saarbrücken.

Er ist Co-Autor des Gutachtens »Modernisierung des Datenschutzrechts«, das 2001 im Auftrag des Bundesministeriums des Innern erstellt worden ist, Herausgeber des »Handbuch Datenschutzrecht«, das 2003 im Beck Verlag erschienen ist, Leiter vieler interdisziplinärer Forschungsprojekte zum Datenschutzrecht in neuen Medien sowie seit 2002 zusammen mit Jörg Tauss (MdB) Organisator der jährlichen Tagung der Friedrich-Ebert-Stiftung zur Modernisierung des Datenschutzrechts.