
Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen

FRIEDEMANN MATTERN

Inhaltsübersicht

- A. Einleitung
- B. Technologietrends
 - I. Das Gesetz von Moore
 - II. Kommunikationstechnik
 - III. Neue Materialien
 - IV. Sensortechnik und RFID
- C. Visionen und Ausprägungen des ubiquitous computing
 - I. Embedded computing
 - II. Wearable computing
 - III. Sensornetze
- D. Konsequenzen
 - I. Anwendungsmöglichkeiten
 - II. Privatsphäre
 - III. Dinge mit Gedächtnis
 - IV. Ethische Fragestellungen
- E. Fazit

A. Einleitung

Der vorliegende Beitrag¹ geht der Frage nach, welche sozialen Konsequenzen und rechtlichen Herausforderungen zu erwarten sind, wenn der gegenwärtige Trend hin zu einer allgegenwärtigen und allumfassenden Informationsverarbeitung weiter anhält. Diese „totale Informatisierung“ der Welt wird auch mit *ubiquitous computing* oder *pervasive computing* bezeichnet – Begriffe, die schon vor einigen Jahren entstanden, aber erst in jüngster Zeit zunehmend in das Bewusstsein der Öffentlichkeit dringen.² Es wird damit der Umstand bezeichnet, dass die Informations- und Computertechnologie nicht nur in

¹ Dieser Beitrag beruht auf früheren Veröffentlichungen des Autors (z.B.: *Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing*. In: Mattern, F. (Hg.), *Total vernetzt – Szenarien einer informatisierten Welt*. Springer-Verlag, 2003, 1–41), insbesondere aber der schriftlichen Fassung des Vortrags *Allgegenwärtige Informationstechnik – Soziale Folgen und Konsequenzen für die Menschenrechte*, gehalten am 16.06.2004 auf dem 1. Internationalen Menschenrechtsforum Luzern (In: Th. Kirchschräger, P. Kirchschräger (Hg.): *Menschenrechte und Terrorismus*, Stämpfli Verlag, Bern, 2004, 313–333). Er verdankt ferner viele Anregungen den Diskussionen im Rahmen des von der Gottlieb Daimler- und Karl Benz-Stiftung geförderten Kollegs „Living in a Smart Environment“.

² Langheinrich, Marc / Mattern, Friedemann (2003) *Digitalisierung des Alltags. Was ist Pervasive Computing?* Aus *Politik und Zeitgeschichte* (B 42), 6–12.

immer mehr Lebensbereiche, sondern zunehmend auch in viele Alltagsgegenstände einzieht – letzteres getrieben von der technischen Entwicklung hin zu immer kleineren und billigeren Mikroprozessoren und Speicherkomponenten sowie einer immer leistungsfähigeren Kommunikationstechnik.

Werden Alltagsdinge informationstechnisch aufgerüstet, dann erhalten sie eine gegenüber ihrem ursprünglichen Zweck erweiterte Funktionalität und können unter Umständen sogar ein „smarter“ beziehungsweise situationsangepasstes Verhalten aufweisen – ohne deswegen schon gleich als „intelligent“ angesehen zu werden. Interessant wird es jedenfalls, wenn gewöhnliche Gegenstände die Möglichkeit bekommen, in drahtloser Weise, also per Funk, miteinander zu kommunizieren und somit zu kooperieren – hier stehen wir erst am Anfang einer spannenden Entwicklung, von der in der Folge berichtet werden soll.

Der allgemeine Trend in der Computertechnik ist hinlänglich bekannt: *schneller, kleiner, billiger*. Tatsächlich hatte noch Mitte der 1970-er Jahre, als der Autor mit seinem Hochschulstudium begann, eine Universität typischerweise nur einen einzigen Computer, der aufgrund seines raumfüllenden Umfangs und seiner für damalige Zeiten hohen Rechengeschwindigkeit von einigen hunderttausend Rechenschritten pro Sekunde auch als „Großcomputer“ bezeichnet wurde. Dieser kostete mehrere Millionen und besaß wenige 100 Kilobyte Speicher. Alle Anwender einer Universität nutzten diesen Computer gemeinsam – dennoch konnte man damit auch damals schon wichtige wissenschaftliche Berechnungen durchführen.

Schon bald darauf, Anfang der 1980-er Jahre, konnten sich dann immer mehr Leute einen eigenen kleinen Computer leisten: Das Zeitalter des *persönlichen Computers* („PC“) war angebrochen, und man steuerte auf ein zahlenmäßiges Verhältnis von 1:1 zwischen Nutzern und Computern zu. Heute hat sich das Verhältnis umgekehrt: Viele von uns besitzen mehrere Mikroprozessoren – eingebaut im Mobiltelefon, in der Armbanduhr und im Auto; dabei ist jeder einzelne leistungsfähiger als ein Großcomputer vor 30 Jahren. Nur deswegen, weil die Computer so viel billiger und kleiner geworden sind, können wir uns überhaupt viele davon leisten. Übrigens aber auch nur deswegen, weil der Energieverbrauch drastisch zurückging – die Stromrechnung eines damaligen Großcomputers möchten wir als Privatperson bestimmt nicht bezahlen!

Dies alles – drastischer Rückgang der Kosten, der Größe und des Energieverbrauchs von Computern – hat im Wesentlichen eine einzige Ursache: der stetige Fortschritt der Mikroelektronik. Der zugrunde liegende Trend ist aber ungebrochen. Wenn die letzten 30 Jahre eine solch dramatische Entwicklung bewirkten, mit Auswirkungen auf unser aller Leben, was ist dann in den nächsten 10 oder 20 Jahren zu erwarten? Und wie könnte sich dies auswirken? Das ist die eigentlich spannende Frage!

In der Folge werden wir auf drei Hauptpunkte eingehen. Im ersten Teil des Beitrags werden einige *Technologietrends* skizziert, die in diesem Kontext von Bedeutung sind. In einem zweiten Teil werden wir dann auf die *Visionen und Ausprägungen* des ubiquitous computing zu sprechen kommen. Schließlich interessiert hier aber vor allem der dritte Teil: Welche *Konsequenzen und Auswirkungen* wird oder kann diese technische Entwicklung haben? Wie ist der Mensch davon betroffen? Kommt hier vielleicht etwas auf uns zu, das zentrale Kategorien unserer Sicht der Welt und unseres Daseins berührt?

B. Technologietrends

Vieles treibt den Fortschritt der Informationstechnik auf ganz unterschiedlichen Ebenen voran: Technische Perfektionierungen von Lasern und Displays, produktivere Methoden zum Erstellen von Software, bessere Programmiersprachen und Betriebssysteme, neue physikalisch-chemische Prozesse für Batterien, innovative Konzepte für die Mensch-Maschine-Interaktion, flexiblere Fertigungsverfahren und noch manches mehr. Das alles wiederum beruht wesentlich auf dem kontinuierlichen Zuwachs an Erfahrung und Wissen sowie dem steten Erkenntnisgewinn der grundlagenorientierten Forschung – Marktmechanismen und allgemeine Wirtschaftsprozesse sorgen dann dafür, dass dies – sofern es ökonomische sinnvoll ist – in einen anwendungsbezogenen Nutzen umgesetzt wird.

Der Fortschritt ist im Detail nicht planbar, und einzelne Entdeckungen geschehen eher zufällig. Dennoch lassen sich auf hoher Ebene, dort wo viele Einzelbeiträge zusammenfließen, klare Trends ausmachen, die über lange Zeit anhalten. Durch Extrapolation solcher Trends kann mit einer gewissen Wahrscheinlichkeit auf die nähere Zukunft geschlossen werden. Nachfolgend sind einige Gebiete aufgeführt, die für den Fortschritt der Informationstechnik wesentlich sind und in denen sich solche Trends erkennen lassen. Damit lässt sich ableiten, welche Möglichkeiten mit der Weiterentwicklung der Informationstechnik insgesamt verbunden sind.

B.I Das Gesetz von Moore

Etwa alle 18 Monate verdoppelt sich aufgrund des technischen Fortschritts in der Mikroelektronik die Leistungsfähigkeit von Prozessoren – bei weitgehend konstanten Kosten. Dieses Phänomen ist unter der Bezeichnung *Gesetz von Moore* bekannt geworden. Auch die Speicherkapazität für Daten und die Übertragungsbandbreite („Geschwindigkeit“) von Computernetzen nimmt in ähnlicher Weise exponentiell zu. Oder anders ausgedrückt: Der Preis für eine bestimmte mikroelektronisch realisierte Funktionalität sinkt schnell und kontinuierlich.

Dieser Trend gilt mit erstaunlicher Präzision schon seit ca. 50 Jahren und ist inzwischen zu einer Art *self-fulfilling prophecy* der Halbleiterindustrie geworden. Experten erwarten, dass es noch mindestens 10 oder 15 Jahre lang so weitergeht – vielleicht sogar noch wesentlich länger. Genaue Aussagen dazu sind aber schwierig, da dies auch von nicht-technischen Faktoren, wie beispielsweise den ökonomischen Randbedingungen, abhängt.

Der stetige Innovationsprozess führt jedenfalls dazu, dass elektronische Komponenten in Zukunft noch wesentlich effizienter, kleiner und billiger werden, womit Computerleistung dann fast im Überfluss vorhanden sein dürfte. Die nach Gebrauch wertlosen Telefonchipkarten oder die als Ersatz für Strichcode-Etiketten dienenden und kurz vor der Masseneinführung stehenden RFID-Chips (elektronische Etiketten, siehe unten) sind erste Hinweise auf die zu erwartenden Myriaden von „Wegwerfcomputern“.

B.II Kommunikationstechnik

Der zweite wichtige Technologiebeitrag für das ubiquitous computing stellt die Kommunikationstechnik dar. Auch hier sind über die Jahre gewaltige Fortschritte und ein Trend hin zu immer höheren Datenraten zu verzeichnen. Wenn wir mittels Glasfasertechnik bald von „Gigabits pro Sekunde“ zu „Terabits pro Sekunde“ kommen, also die Menge der übertragbaren Information pro Zeiteinheit vertausendfachen, dann regt das niemanden mehr richtig auf – man erwartet dies förmlich! Dabei bedeutet „Gigabits pro Sekunde“ schon, dass in einer Sekunde eine Milliarde Informationseinheiten (Bits) übermittelt werden können (der Text dieses Beitrags also innerhalb von nur einer Millisekunde über die Leitung huscht), und bei „Terabits pro Sekunde“ sind es noch tausend Mal mehr!

Besonders relevant für das ubiquitous computing ist die drahtlose Kommunikation. Das Mobilfunknetz für Handys sowie der drahtlose Internetzugang via WLAN und Bluetooth sind heute Standard – mit bereits entwickelten und kurz vor dem kommerziellen Einsatz befindlichen neuen Technologien wie „Ultra Wide Band“ (UWB) und ZigBee wird erreicht, dass die Kommunikationsmodule noch kleiner werden können, die in die portablen Geräte eingebauten Akkumulatoren nur noch ganz selten aufgeladen werden müssen und noch mehr Daten noch schneller „durch die Luft“ transportiert werden können. Die fernere Zukunft schließlich lässt noch mehr an Leistungssteigerung erwarten.

Spannend sind auch Entwicklungen im Bereich von „Body Area Networks“ – hier kann der menschliche Körper selbst als Medium zur Übertragung von Signalen extrem geringer Stromstärken genutzt werden. Allein durch Anfassen eines Gerätes oder Gegenstandes kann diesem dann eine eindeutige Identifikation übermittelt werden, die beispielsweise von der eigenen Armbanduhr stammt; auf diese Weise könnten zukünftig Überprü-

fungen von Zugangsberechtigungen, die Personalisierung von Geräten oder die Abrechnung von Dienstleistungen erfolgen.

An dieser Stelle sei gestattet, kurz mit einigen Zitaten aus einem mittlerweile fast 100 Jahre alten Buch *Die Welt in 100 Jahren*³ auf die früher gehegten Erwartungen an die Möglichkeiten der Telekommunikation einzugehen. Das Buch beschreibt eine Welt, in der wir heute eigentlich leben müssten – wenn die Vorhersagen über diesen langen Zeitraum einigermaßen zutreffend waren! Dabei beschränken wir uns hier auf das Kapitel *Das drahtlose Jahrhundert*.

Was also hat man damals für die heutige Zeit prophezeit? Erstaunliches, wenn man sich der Tatsache bewusst ist, dass zu jener Zeit sowohl die Funk- als auch die Telefontechnik erst rudimentär entwickelt waren. Es heißt dort nämlich: „*Es wird jedermann sein eigenes Taschentelephon haben, durch welches er sich, mit wem er will, wird verbinden können, einerlei, wo er auch ist, ob auf der See, ob in den Bergen, dem durch die Luft gleitenden Aeroplan oder dem in der Tiefe der See dahinfahrenden Unterseeboot.*“ Zwar hat man das mit dem Unterseeboot noch nicht erreicht, ansonsten aber beschreibt dies unser Handy-Zeitalter doch recht genau!

Weiter heißt es: „*Die Bürger jener Zeit werden überall mit ihrem drahtlosen Empfänger herumgehen, der irgendwo, im Hut oder anderswo angebracht sein wird.*“ Hüte sind etwas aus der Mode gekommen, daher scheidet diese Möglichkeit heutzutage aus – aber wenn wir das Handy nicht einfach in der Hosentasche stecken haben, dann vielleicht in der Handtasche oder einem modischen Gürtelhalter. Die Nutzungsmöglichkeiten eines drahtlosen Taschentelephons schienen damals jedenfalls phantastisch und fast unbegrenzt: „*Monarchen, Kanzler, Diplomaten, Bankiers, Beamte und Direktoren werden ihre Geschäfte erledigen können, wo immer sie sind.*“ Dass sich zwölfjährige Schulmädchen über zwei Meter Entfernung eine Textnachricht via SMS oder mit einem Fotohandy sogar einen Schnappschuss zusenden, war seinerzeit allerdings wohl doch jenseits des sinnvoll Vorstellbaren. Dennoch sollte nicht nur die Geschäftswelt von den Möglichkeiten der drahtlosen Kommunikation profitieren. Da auch Lokomotivführer drahtlos kommunizieren können, ist – so heißt es weiter in diesem Buch – eine Kollision von Zügen auf einer eingleisigen Strecke forthin natürlich „ganz unmöglich“.

Auch alltägliche Verrichtungen werden von der videobasierten Kommunikationstechnik revolutioniert: „*Überhaupt wird das Einkaufen zu jener Zeit ein noch viel größeres Vergnügen sein, als jetzt. Man wird einfach von seinem Zimmer aus alle Warenhäuser durchwandern können und in jeder Abteilung Halt machen, die man eingehender zu besichtigen oder wo man etwas auszuwählen wünscht... Alle diese Wunder der drahtlosen Telegraphie wer-*

³ Brehmer, Arthur (Hg.) (1910) *Die Welt in 100 Jahren*. Berlin, Verlagsanstalt Buntdruck GmbH.

den das kommende Zeitalter zu einem großartigen, unglaublichen machen.“ Fast meint man, die Melancholie des Autors im letzten Satz zu spüren: Dass er dieses großartige Zeitalter nicht mehr selbst wird erleben können!

Und weiter: *„Nirgends, wo man auch ist, ist man allein. Überall ist man in Verbindung mit allem und jedem. Auch auf die Ehe und die Liebe wird der Einfluß der drahtlosen Telegraphie ein außerordentlicher sein. Künftighin wird sich die leibliche Gattin stets davon überzeugen können, was ihr Herr Gemahl treibt; aber auch der Herr Gemahl wird ganz genau wissen, wie und ob seine Gattin nur an ihn denkt. Liebespaare und Ehepaare werden nie voneinander getrennt sein, selbst wenn sie Hunderte und Tausende Meilen voneinander entfernt sind. Sie werden sich immer sehen, immer sprechen, kurzum, es wird die Glückszeit der Liebe angebrochen sein.“*

Aus heutiger Sicht lässt sich kaum noch feststellen, ob eine gewisse Ironie in diesen Textzeilen mitschwingt. Ist es denn wirklich erstrebenswert, wenn der eine stets wissen kann, was der andere treibt? Wir kommen darauf noch zurück.

B.III Neue Materialien

Kommen wir nun zur dritten wichtigen Entwicklung, den neuen Materialien. Schon immer haben Werkstoffe ganze Zeitalter geprägt, denken wir nur an Bezeichnungen wie *Steinzeit* oder *Eisenzeit*. Die zweite Hälfte des letzten Jahrhunderts war wesentlich durch Silizium bestimmt – das Grundmaterial der Halbleiterindustrie und der Stoff, aus dem der Mikroprozessor besteht.

Jetzt aber, zu Beginn des einundzwanzigsten Jahrhunderts, zeichnet sich etwas Neues ab: Es sieht so aus, als ob Polymere, also „Plastik“, eine ganz wesentliche Rolle spielen werden und Dinge erlauben, die man früher nie erwartet hätte! Nicht zuletzt wird es dadurch möglich, dass Computer recht ungewöhnliche Formen annehmen – diese können sich z.B. als papierähnliche Plastikfolien materialisieren.

Als Beispiel sei hier kurz angedeutet, wie die in Entwicklung befindliche *elektronische Tinte* funktioniert, die auf eine sehr dünne Plastikfolie aufgetragen wird. Hier gibt es verschiedene technische Möglichkeiten, eine davon beruht auf folgendem Prinzip: In kleinen, submillimeter großen Kapseln „schwimmen“ weiße und schwarze, elektrisch unterschiedlich geladene Farbpartikel. Legt man an einer Stelle der Folie eine positive oder negative Spannung an, dann fließen entweder die weißen oder die schwarzen Farbpigmente nach oben und erzeugen an dieser Stelle einen kleinen Punkt in der entsprechenden Farbe. Auf diese Weise kann dynamisch etwas geschrieben und später wieder gelöscht werden. Idealerweise sollte sich die Folie dann anfühlen wie Papier – ganz so weit ist man allerdings mit der Entwicklung noch nicht. Immerhin existieren jedoch schon Prototypen. Diese haben noch diverse Mängel was z.B. Haltbarkeit, Pixelgröße oder Preis betrifft, an deren Be-

hebung man aber natürlich arbeitet. Die Bedeutung für die Praxis, wenn irgendwann einmal Papier, ein uns auch kulturell wohl vertrautes und klassisches Medium, quasi zum Computer mutiert oder umgekehrt der Computer als Papier daherkommt, kann kaum hoch genug eingeschätzt werden!

B.IV Sensortechnik und RFID

Schließlich soll als letztes hier betrachtetes Gebiet auf die Sensortechnik eingegangen werden. Sensoren sind „Fühler“, die Eigenschaften der Umgebung (Temperatur, Feuchtigkeit, Stärke eines Magnetfeldes, Anwesenheit von bestimmter Strahlung etc.) wahrnehmen und dies in elektrischer Form weitermelden. Sensoren stellen damit gewissermaßen die „Sinnesorgane“ von Computern dar.

Bei der Sensortechnik wurden in den letzten Jahren bedeutende Fortschritte erzielt. Autos z.B. enthalten eine Vielzahl unterschiedlicher Sensoren zur Messung von Umgebungsparametern zwecks dynamischer Optimierung der Motorwerte; aber auch der Airbag enthält einen Sensor, der auf den typischen Stoß bei einer Kollision reagiert.

In etwas verallgemeinerter Form kann man auch Kameras zu den Sensoren rechnen – diese sind ja so klein geworden, dass sie mittlerweile in viele Handys eingebaut werden. Vor allem aber sind sie auch so billig, dass sich nicht nur James Bond eine Spezialanfertigung leisten kann. Auch GPS-Empfänger und andere Lokalisatoren stellen in gewisser Weise Sensoren für den geographischen Ort dar – diese sind einschließlich der notwendigen Antennen nicht mehr viel größer als eine Kreditkarte.

Als Beispiel sollen hier „Identitätssensoren“ etwas näher betrachtet werden, die auf dem Prinzip der *Radio Frequency Identification* beruhen, abgekürzt RFID. Die RFID-Technik ist in letzter Zeit in den Medien kontrovers diskutiert worden; wir kommen darauf gleich zurück.

Eine vereinfachte Form der RFID-Technologie kennt man von Kaufhäusern und Boutiquen, wo sie zum Diebstahlschutz eingesetzt wird: Antennen in den „Türschleusen“ senden ein Hochfrequenzsignal aus; dieses nimmt der in die Verpackungen der Produkte integrierte Chip über eine kleine Antenne wahr und schickt eine Antwort zurück. Eine eigene Batterie oder sonstige Energiequelle auf dem Chip ist dabei nicht nötig, da er nach dem Prinzip der magnetischen Induktion gleichzeitig auch mit Energie aus dem Sendesignal versorgt wird.

Im Falle des Diebstahlschutzes geht es bei der zurückgesendeten Antwort nur um einen binären Wert *bezahlt* oder *nicht bezahlt*. Allgemeiner lässt sich aber eine eindeutige Seriennummer aus dem RFID-Chip ermitteln, und man kann sogar in umgekehrter Richtung Informationen bis zu einigen hundert Bits „durch die Luft“ auf den Chip schreiben. Diese Informationsübertragung geschieht dabei im Sekundenbruchteil und über Entfernungen von bis zu

einigen wenigen Metern. RFID-Chips inklusive der papierdünnen flexiblen Antenne kosten derzeit mit fallender Tendenz zwischen 10 Cent und 1 Euro pro Stück und lassen sich schon recht klein fertigen.

Was man mit solchen RFID-Chips anstellen kann, zeigt ein „smartes Kartenspiel“, das an der ETH Zürich entwickelt wurde. Dabei trägt jede Spielkarte einen kleinen RFID-Chip. Unter dem Spieltisch ist eine größere Antenne montiert, die registriert, welche Karte jeweils ausgespielt wird. Dadurch kann die „intelligente“ Umgebung den Spielverlauf automatisch nachvollziehen und eventuelle Regelwidrigkeiten erkennen, die Spielpunkte zusammenzählen und den Gewinner ermitteln. Es ist aber noch mehr möglich: In drahtloser Weise werden den Mitspielern auf einen „persönlichen digitalen Assistenten“ (PDA) spezifische Informationen zum Spielverlauf übermittelt. Der PDA ist dabei natürlich nur für den jeweiligen Spieler einsehbar. Anfänger können so z.B. auf die in der konkreten Situation spielbaren Karten aufmerksam gemacht werden. Für Außenstehende sieht das Ganze wie Magie aus – aber unsichtbare Technik ist ja oft „implementierte Magie“!

Die RFID-Technik wurde natürlich nicht für solche „Spielereien“ entwickelt. Vorangetrieben wird sie von Anwendungsmöglichkeiten im Bereich der Logistik, wo aufgrund des großen Warenvolumens bereits kleinste Optimierungen erhebliche Einsparungen mit sich bringen: Wenn Produkte ihre Identität jedes Mal automatisch preisgeben, wenn sie das Tor einer Lagerhalle oder die Laderampe eines LKW passieren, dann kann ohne manuelles Zutun eine lückenlose Verfolgung der Warenströme über die gesamte Lieferkette hinweg sichergestellt werden.

Große Hoffnungen setzen Logistikbranche und Einzelhandel auch auf den Ersatz des Strichcodes auf Supermarktwaren durch RFID-Chips. Idealerweise kann man als Kunde dann mit seinem Einkaufswagen durch das Checkout-Gate fahren und bekommt sofort – oder einmal im Monat – die Rechnung präsentiert. Bis Supermarktkassen tatsächlich obsolet werden, sind allerdings noch einige technische und organisatorische Probleme zu lösen!

Viele weitere Anwendungsmöglichkeiten sind für solche automatischen Identifikationstechnologien denkbar. Enthält die Bordkarte eines Flugreisenden beispielsweise einen RFID-Chip, dann kann beim Passieren geeignet instrumentierter Stellen automatisch festgestellt werden, in welchem Flughafenbereich er sich befindet. Er braucht dann nicht mehr überall per Lautsprecher ausgerufen zu werden, und die Fluggesellschaft kann entscheiden, ob es sich lohnt, die Maschine noch einige Minuten warten zu lassen – nämlich dann, wenn die Person (bzw. genauer: die Bordkarte mit dem Chip) nicht mehr weit vom Gate entfernt ist und es sich um einen First-Class-Passagier handelt... Oder: Können RFID-Chips von einer Waschmaschine gelesen werden, dann kann sich diese automatisch auf die Wäsche einstellen. Eine nette Einsatzmöglichkeit stellen auch RFID-Chips im Abfall dar; hier kann ein Produkt der Müllsortieranlage in einer „letzten“ Willensmitteilung kund-

tun, aus was es besteht und wie seine Überreste behandelt werden sollen. Ob solche Dinge wirklich realisiert werden, wenn RFID-Chips irgendwann einmal allgegenwärtig sind, und ob die Menschen dies dann auch haben wollen, lässt sich allerdings kaum vorhersagen.

Vorerst beherrscht beim Thema RFID die mögliche Gefährdung der Privatsphäre die Diskussion in der Öffentlichkeit.⁴ Man misstraut den Supermärkten, die Waren mit Funketiketten anbieten, und unterstellt ihnen heimliches Datensammeln. Ferner möchte man nicht, dass irgendjemand, ausgestattet mit einem Handscanner, erfahren kann, was man bei sich trägt, weil ihm die Produkte ihre Identität preisgeben. Auch letztere Sorgen sind ernst zu nehmen, unabhängig davon, ob derartige Szenarien wahrscheinlich oder eher unwahrscheinlich erscheinen und ob sie technisch überhaupt realistisch sind.⁵ Jedenfalls hat das versuchsweise Anbringen von RFID-Chips an (bisher erst wenigen) Supermarktprodukten bereits zu Protesten und Demonstrationen geführt, und auch Gesetzesvorlagen wurden in den USA (letzten Endes allerdings erfolglos) schon eingebracht. Im Wesentlichen geht es bei den Datenschutzinitiativen darum, dass RFID-Chips nicht „heimlich“ an Verkaufswaren angebracht werden, dass die Kunden zustimmen müssen und dass die RFID-Chips außerhalb des Ladens nicht mehr aktiv sind. Man wird sehen müssen, bis zu welchem Grade solche Forderungen realistisch sind bzw. tatsächlich im Interesse der Kunden liegen (die damit eventuell auf gewisse Vorteile verzichten müssten) und Aussicht auf Erfolg haben. Im Deutschen Bundestag wurde eine Kleine Anfrage⁶ der FDP nach den Gefahren des Missbrauchs von RFID-Chips von der Bundesregierung jedenfalls damit beantwortet⁷, dass mit RFID eine heimliche Erstellung umfassender Bewegungsprofile nach dem gegenwärtigen Stand der Technik praktisch ausgeschlossen sei und ein ergänzender datenschutzrechtlicher Regelungsbedarf nicht erkennbar sei.

Auf den allgemeinen Aspekt des Datenschutzes und der Gefährdung der Privatsphäre bei ubiquitous computing kommen wir unten noch zurück.

⁴ Thiesse, Frédéric / Fleisch, Elgar (2005) *Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung*. In: Fleisch, Elgar; Mattern, Friedemann (Hg.), *Das Internet der Dinge*. Springer-Verlag.

⁵ Langheinrich, Marc (2005) *Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie*. In: Fleisch, Elgar / Mattern, Friedemann (Hg.), *Das Internet der Dinge*. Springer-Verlag.

⁶ Deutscher Bundestag (2004) *Technologie der Radio Frequency Identification*. Drucksache 15/3025.

⁷ Deutscher Bundestag (2004) *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Rainer Brüderle, Ernst Burgbacher, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/3025 – Technologie der Radio Frequency Identification*. Drucksache 15/3190.

C. Visionen und Ausprägungen des ubiquitous computing

Mit den im letzten Kapitel skizzierten technischen Entwicklungen wird eine neue Ära der Computeranwendung eingeläutet: Drahtlos kommunizierende Prozessoren und Sensoren können aufgrund ihrer geringen Größe und ihres vernachlässigbaren Preises und Energiebedarfs bald in viele Gegenstände integriert oder anderweitig in die Umwelt eingebracht werden. Informationsverarbeitung gekoppelt mit Kommunikationsfähigkeit dringt so fast überall ein, sogar in Dinge, die zumindest auf den ersten Blick keine elektrischen Geräte darstellen. Damit sind auch die technischen Voraussetzungen für eine „totale Informatisierung“ der Welt geschaffen.

Früh erkannt hat das Potential, das im nachhaltigen Fortschritt der Mikroelektronik und Informationstechnik liegt, Mark Weiser, seinerzeit leitender Wissenschaftler am Xerox-Forschungszentrum im Silicon Valley. Basierend auf seinen eigenen Entwicklungen propagierte er schon 1991 in seinem visionären Artikel *The Computer for the 21st Century*⁸ den allgegenwärtigen Computer, der unsichtbar und unaufdringlich den Menschen bei seinen Tätigkeiten unterstützt und ihn von lästigen Routineaufgaben weitestgehend befreit. Weiser stellte seinerzeit die These auf, dass das einundzwanzigste Jahrhundert dadurch geprägt sein wird, dass die *kleine* Technik – insbesondere die Computertechnik – in den Alltag einzieht und sich dort unsichtbar macht. Tatsächlich kann man derzeit ja erkennen, dass dem Kleinen – „Mikro“, „Nano“, „Bio“ etc. – viel Aufmerksamkeit zukommt, nachdem das letzte Jahrhundert eher durch Großtechnologie geprägt war. Nun erfordert aber Großtechnologie wie die Atomtechnik oder die Eroberung des Weltraums nicht nur viel Geld, sondern auch einen nachhaltigen gesellschaftlichen Konsens – hier hat es die quasi unsichtbare und evolutionär daherkommende kleine Technik besser, ganz abgesehen davon, dass sich Kleines oft mit weniger Aufwand replizieren und wesentlich schneller (und vielleicht auch in selbstorganisierter und damit „demokratischerer“ Weise) verbreiten lässt als Großes. Die Technik des Kleinen sollte sich also viel leichter durchsetzen als die Großtechnik, wenn sie erst einmal vorhanden ist.

Die Aussage von Marc Weiser „*in the 21st century the technology revolution will move into the everyday, the small and the invisible*“ lässt sich auf verschiedene Art interpretieren. Kleine und preiswerte Prozessoren, Sensoren, Speicher und Kommunikationsmodule lassen sich einerseits in Alltagsgegenstände integrieren, was als *embedded computing* bezeichnet wird. Wenn man sie am Körper oder in der Kleidung trägt, dann spricht man eher von *wearable computing*. Stattet man die Umwelt damit aus, etwa um die Umgebung zu beobachten, dann erhält man schließlich *Sensornetze*. Auf alle drei Aspek-

⁸ Weiser, Mark (1991) *The Computer for the 21st Century*. Scientific American 265(3), 66–75.

te soll im Folgenden kurz eingegangen werden. Beginnen wir mit dem embedded computing.

C.I Embedded computing

Möchte man Alltagsdinge „smart“ machen und sie mit der Fähigkeit ausstatten, Information zu verarbeiten, dann gehört dazu zunächst ein Mikroprozessor. Einfache Prozessoren, die nicht höchste PC-Leistung erzeugen müssen, können billig und klein hergestellt werden. Damit die Information weitergeleitet werden kann, braucht man zusätzlich noch drahtlose Kommunikationsmodule, womit sich benachbarte Gegenstände zu Netzen zusammenschließen können. Damit dies alles überhaupt sinnvoll ist, müssen die Gegenstände Information aus ihrer Umgebung aufnehmen, wofür Sensoren eingesetzt werden.

Die verschiedenen Basistechnologien, nämlich Analog-, Digital- und Hochfrequenztechnologie der Sensoren, Prozessoren und Kommunikationsmodule stellen 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 – an einen Menschen, an ein informationstechnisches System oder an andere so ausgestattete smarte Dinge.

Auf diese Weise können Alltagsgegenstände kommunizieren und sich beispielsweise über die wahrgenommenen Umgebungsbedingungen austauschen, wodurch die Grundlage für eine Kooperation von Dingen miteinander gelegt wird. Salopp ausgedrückt entstehen so „smarte“ Gegenstände. Diese können sich gewisse Vorkommnisse merken – wenn sie mit einem Lokationssensor ausgestattet sind, z.B. wo sie schon überall waren. Sie können sich – bei geeigneter Programmierung – auch kontextbezogen verhalten. Ein Rasensprinkler würde z.B. neben den Feuchtigkeitssensoren im Boden auch die Wettervorhersage im Internet konsultieren, bevor er sich entscheidet, den Rasen zu wässern.

Wozu aber sollten z.B. eine Armbanduhr und eine Kreditkarte miteinander kommunizieren? Auch dies ist nicht ganz so absurd, wie es auf den ersten Blick erscheinen mag. Dazu stellt man sich vor, dass beide mit winzigen Beschleunigungssensoren versehen sind, die messen können, in welcher Weise der jeweilige Gegenstand geschüttelt wird. Schüttelt man nun beide zusammen (indem man die Kreditkarte in der Hand mit der Armbanduhr hält), so würden beide ihr jeweiliges Schüttelmuster per Funk in der näheren Umgebung verbreiten. Durch Empfang eines weitgehend identischen Musters eines anderen Gegenstandes weiß der Empfänger dann, dass ein gemeinsamer

„Schüttelkontext“ vorliegen muss.⁹ Im skizzierten Szenario würde (durch gemeinsames Schütteln) die Kreditkarte auf die Armbanduhr geprägt und fortan nur noch funktionieren, wenn sie in unmittelbarer Nähe „ihrer“ Armbanduhr ist. Eine verlorene oder gestohlene Kreditkarte würde ihren Dienst verweigern. Eine neue Kreditkarte kommt daher in Zukunft vielleicht mit der Anweisung „Vor erstmaligem Gebrauch gut schütteln!“.

C.II Wearable computing

Zurück zur Vision von Mark Weiser. Betrachten wir kurz die zweite Ausprägung der „totalen Informatisierung“, das wearable computing. Dies ist aufgrund der bildlich einprägsamen Cyborg-Phantasien ein dankbares Gebiet für die Medien, aber auch mit etwas weniger Phantasie kann man sich leicht vorstellen, dass in Zukunft immer mehr elektronisches Gerät in miniaturisierter Form in Kleidung, Armbanduhren und Schmuckstücke eingebaut werden kann. Handy-Mikrophone und kleine Displays lassen sich schon heute als leicht zu tragende Accessoires nutzen – vor wenigen Jahren wäre das noch schier unvorstellbar gewesen. In der Erprobung befinden sich aber auch schon sogenannte 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!

Solche Brillen eröffnen nun ganz neue Möglichkeiten zur Informationsdarstellung – Computer und Fernseher könnten dann z.B. auf ihre Bildschirme verzichten. Richtig interessant wird es aber, wenn der Brillenträger Informationen eingeblendet bekommt, die in der jeweiligen Situation für ihn nützlich sind. Dies hat Mahadev Satyanarayanan auf nette (und vielleicht nicht so ganz ernst gemeinte) Weise einmal wie folgt beschrieben¹⁰, wobei er davon ausgeht, dass neben einer kleinen Kamera, die man bei Foto-Handys ja bereits findet, zukünftig auch ein Softwaresystem zur visuellen Objekterkennung vorhanden ist: „*You could wear a pair of glasses with a small amount of face recognition built-in, look at a person, and his name would pop up in a balloon above his head. You could know instantly who the person is, even if you don't immediately recognize him. I look at my tree, and a little balloon*

⁹ Holmquist, Lars Erik / Mattern, Friedemann / Schiele, Bernt / Alahuhta, Petteri / Beigl, Michael / Gellersen, Hans-Werner (2001) *Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts*. Proc. Ubicomp 2001, LNCS 2201, Springer-Verlag, 116–122.

¹⁰ Satyanarayanan, Mahadev (2001) *Interview: M. Satyanarayanan on Mobile and Pervasive Computing*. IEEE Distributed Systems Online, Vol. 2, No. 6, http://ads.computer.org/dsonline/0106/departments/int0106_print.htm.

pops up saying, 'Water me,' I look at my dog, it says, 'Take me out,' or I look at my wife, it says, 'Don't forget my birthday!' "

C.III Sensornetze

Gehen wir nun noch auf die letzte hier betrachtete Ausprägung der Vision ein, die Sensornetze. Dabei geht man davon aus, dass eine große Zahl hochgradig miniaturisierter Sensoren großflächig in die Umwelt eingebracht wird, indem diese im Extremfall z.B. aus einem Flugzeug abgeworfen werden. Die Aufgabe der Sensoren besteht darin, ihre jeweilige unmittelbare Umgebung zu beobachten.

Die Sensoren können sich bei Bedarf drahtlos mit benachbarten Sensoren vernetzen, ihre Arbeit untereinander abstimmen und relevante Erkenntnisse austauschen. Wird es bei einem Sensor z.B. heiß, kurze Zeit später bei einem benachbarten Sensor, und wieder etwas später bei einem dritten Sensor, so lässt sich daraus auf ein Feuer sowie dessen Ausbreitungsrichtung und -geschwindigkeit, etwa bei einem Waldbrand, schließen.

Prototypen solcher Sensornetze existieren bereits, allerdings steht man hier erst am Anfang der technischen Entwicklung. Beherrscht man jedoch eines Tages die Technik zur massenweisen Herstellung kleiner und energieeffizienter Sensoren, die sich automatisch flexibel vernetzen, dann lassen sich mit ihnen vielfältige Phänomene der Welt in bisher nie da gewesener Genauigkeit beobachten. Durch die geringe Größe und dadurch, dass keine physische Infrastruktur (Verkabelung, Stromanschlüsse etc.) benötigt wird, kann die Instrumentierung in flexibler und nahezu unsichtbarer Weise geschehen. Das Umweltmonitoring stellt genauso eine Anwendung dar wie der militärische Bereich, welcher die Forschung derzeit stark vorantreibt. Auch Infrastruktursysteme, Verkehrssysteme und Fabrikationsprozesse könnten von einem genauen und „unaufdringlichen“ Monitoring profitieren.

Kritisch wird es allerdings dann, wenn mit Sensornetzen in indirekter oder gar direkter Weise Menschen beobachtet werden: Schließlich handelt es sich bei den Sensoren um nahezu unsichtbare, aber äußerst mitteilsame „Spione“. Wenn diese ein billiges Massenprodukt werden, dann lässt sich der Einsatz nicht kontrollieren und ein Missbrauch kaum verhindern.

D. Konsequenzen

Der weiter anhaltende Technologietrend zeigt eindeutig in Richtung einer umfassenden Informatisierung der Welt. Über kurz oder lang dürften damit einige der geschilderten Visionen so oder zumindest in ähnlicher Weise realisierbar werden: Kaum sichtbare Sensoren beobachten die Umwelt (und damit vielleicht auch uns), und Alltagsgegenstände werden „smart“ – sie

wissen, wo sie sich gerade befinden, welche anderen Dinge oder Personen in der Nähe sind, was in der Vergangenheit mit ihnen geschah und teilen ihre Erkenntnisse anderen Gegenständen mit. Welche Auswirkungen kann dies alles nun auf uns Menschen haben? Und was für Konsequenzen sind daraus zu ziehen?

D.I Anwendungsmöglichkeiten

Befassen wir uns zunächst damit, welche Anwendungsmöglichkeiten sich für Alltagsdinge ergeben, die „smart“ sind und miteinander kommunizieren. Hierzu soll vorab eine bewusst provokative Geschichte der Unternehmensberatung Accenture¹¹ nacherzählt werden.¹² Es geht um die Frage, was wäre, wenn smarte Barbie-Puppen selbständig, quasi nach eigenem Gutdünken, Geld ausgeben könnten, um sich neue Kleidchen zu kaufen: „*In the future the customers of any business will not just be people. Objects may manage a budget and have the ability to make their own decisions... The doll has inexpensive and embedded electronics that allows it to see associated products and accessories and remember them. In this way the doll can be constantly, anonymously shopping.*“

Wenn eine solche Puppe etwa zur Puppe der Freundin mitgenommen wird, dann erfährt die eine, was die andere Puppe für Kleidchen hat. Wieder daheim, kann sie sich drahtlos mit dem PC ihrer Besitzerin verbinden und über das Internet automatisch Einkäufe tätigen. Was sie einkauft, kann vom Kontext und der aktuellen Situation anhängen. Vielleicht hat das Kind, dem die Puppe gehört, darauf dann doch auch noch einen gewissen Einfluss: „*What the doll decides to purchase will be based on a variety of information. Such as what she has already, what promotions or discounts are available, how much money she has in her electronic wallet or even what the child wants.*“

Das geschilderte Szenario ist nicht ganz so absurd, wie es zunächst klingt. Viele Geschäftstransaktionen könnten in Zukunft tatsächlich ohne menschliches Zutun direkt von Ding zu Ding ablaufen – man denkt beim *silent commerce* zum Beispiel an Kopierer, die in eigener Verantwortung Papier nachbestellen.

Generell kann man sich hinsichtlich der Anwendungsmöglichkeiten smarter Dinge viel Unsinniges, aber auch einiges Sinnvolles vorstellen, was Menschen nutzt oder ihnen zumindest Spaß macht. Zum Beispiel könnte ein Auto das andere auf der Gegenfahrbahn vor einem Stau warnen. Oder mein Mobiltelefon könnte sich daran erinnern, wann und wo es zuletzt in unmittelbarer

¹¹ Accenture Technology Labs (2001) *Silent Commerce*. www.accenture.com/xd/xd.asp?it=enweb&xd=services/technology/vision/silent_commerce.xml.

¹² Maeder, Thomas (2002) *What Barbie Wants, Barbie Gets*. Wired Magazine 10(1), 6.

Nähe meines Schlüsselbundes war. Ferner mag eine Mülltonne neugierig auf die Recyclingfähigkeit ihres Inhaltes sein, ein Arzneischrank mag um die Verträglichkeit seiner Medikamente und deren Haltbarkeit besorgt sein, und eine Wohnungsheizung könnte mit dem Auto oder anderen persönlichen Gegenständen der Bewohner „konspirieren“ wollen, um zu erfahren, ob mit deren baldiger Rückkehr zu rechnen ist.

Vor allem Lokalisierungstechnologien besitzen ein hohes Anwendungspotential. Wird man in Zukunft einen verlorenen Gegenstand fast immer wiederfinden, weil dieser stets weiß, wo er ist, und er dies bei Bedarf mitteilen kann? Noch sind Lokalisierungsmodule, die beispielsweise auf dem GPS-System beruhen, für viele Anwendungen zu groß, zu teuer, zu ungenau und zu energiehungrig. Bei allen vier Parametern erzielt man allerdings kontinuierliche Fortschritte, und für größere und wertvolle Dinge wie beispielsweise Mietautos rechnet sich ihr Einsatz schon heute. Es ist daher absehbar, dass sich in Zukunft für viele Dinge eine Art „Fahrtenschreiber“ realisieren lässt: Weiß ein Gegenstand, wo er sich befindet, dann braucht er dies nur regelmäßig zusammen mit der momentanen Uhrzeit abzuspeichern – im Nachhinein lässt sich dann die „Lebensspur“ des Gegenstandes einfach rekonstruieren. Durch den Abgleich verschiedener solcher Lebensspuren kann der gemeinsame Kontext verschiedener Dinge ermittelt werden, oder es kann über diese Historie einfach Zugang zu damit verbundenen Informationen (z.B. das Hotel, in dem sich eine ortsbewusste Reisetasche befand) erlangt werden.

Würden kooperierende smarte Alltagsdinge einen ökonomischen Mehrwert ergeben? Hierzu nur ein paar kurze Hinweise. Wenn Produkte jederzeit Auskunft geben können, wo im Produktionsprozess oder der Lieferkette sie sich befinden, ist das bestimmt oft von Vorteil für Hersteller und Lieferanten. Auch zu erfahren, wie intensiv ein Produkt durch den Kunden genutzt wird, ist für den Hersteller nützlich – er könnte dem Kunden dann zum Beispiel passend und rechtzeitig vor der Konkurrenz etwas Neues anbieten...

Theoretisch wäre sogar denkbar, dass die Milch im Supermarkt dynamisch ihren Preis ändert: Wenn sie älter wird, senkt sie ihren Preis, wenn sie einsam im Supermarkt wird, kann sie ihn dagegen erhöhen. Dies klingt ziemlich absurd und würde so von den Kunden vermutlich nicht akzeptiert. Wie wäre es aber mit dynamischen Autoversicherungen, die ihre Prämie davon abhängig machen, ob schnell oder langsam gefahren wird, ob gefährliche Überholmanöver durchgeführt werden, in welchen Gegenden der Wagen abgestellt wird und auf was für Straßen man fährt?

Durch Ortungssysteme wie GPS ist jedenfalls feststellbar, wo sich ein Auto befindet, und dies kann, zusammen mit der Fahrgeschwindigkeit und weiteren Parametern, per Mobilkommunikation jederzeit an die Versicherung gemeldet werden. Auf Testmärkten wurden dynamische Autoversicherungen, die sich in ihrem Preis nach dem Fahrverhalten und der Fahrleistung richten, bereits ausprobiert – viele Leute waren bereit, für eine 25-prozentige Reduk-

tion des Tarifs die Versicherung wissen zu lassen, wo man sich mit dem Auto befindet, und damit ein Stück ihrer Privatsphäre aufzugeben.

D.II Privatsphäre

Wie also steht es um die Privatsphäre? Schon im Internet – für das die ursprünglichen Datenschutzgesetze ja gar nicht gemacht wurden – gibt es einige Probleme in dieser Hinsicht (z.B. Bildung von Interessensprofilen durch Erfassung von Mausklicks und besuchten Web-Seiten, Weitergabe solcher Daten und die Verknüpfung mit anderen Datenbeständen), da fast jede Handlung in diesem viele Lebensbereiche erfassenden Cyberspace Datenspuren hinterlässt, die ausgewertet werden könnten.¹³ Das ist aber kein Vergleich zu dem, was potentiell droht, wenn kleinste Sensoren an Alltagsdingen ihre Beobachtung weitermelden. Dem Internet können wir uns noch entziehen, indem wir den PC abschalten; der realen Welt können wir aber nicht so einfach entfliehen: Smarte Gegenstände und sensorbestückte Umgebungen sind fast immer aktiv und häufen eine Unmenge von Daten an, um den Nutzern jederzeit ihre Dienste anbieten zu können. Vor allem wissen wir nie genau, ob wir bei irgendwelchen Handlungen beobachtet werden. Eine einzelne Beobachtung mag für sich genommen auch harmlos sein – aber wenn verschiedene Beobachtungen zusammengeführt werden, kann dies u.U. eine folgenschwere Verletzung der Privatsphäre nach sich ziehen.

Während sich bisher die informationelle Überwachung einer Person klar abgrenzbar auf die Benutzung von PC und Internet beschränkt, wird es in einer Welt voll Sensoren und smarter Alltagsgegenstände oft gar keine klare Unterscheidung zwischen dem „Online“ und dem „Offline“ mehr geben. Mit dem ubiquitous computing gelangt unweigerlich auch die Verarbeitung personenbezogener Daten in die Alltagsgegenstände der körperlichen Welt. Laut Roßnagel und Müller¹⁴ stellt dies nach dem Internet (potentiell vollständige Erfassung nur eines Ausschnitts des täglichen Lebens) eine qualitativ neue Stufe durch potentiell vollständige Erfassung potentiell aller Lebensbereiche dar. Somit verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell, denn wo vorher nur ein relativ begrenzter Aspekt einer Person erfassbar war, offenbart sich dann ein weitaus detaillierteres Bild über die Interessen, die Neigungen, die allgemeine Verfassung und auch über die Schwächen einer Person. Da auf diese Weise, oft durchaus ungewollt und quasi als Nebenprodukt der Verwendung bequemer oder qualitätssteigernder Dienste, leicht individuelle Aktivitätsprotokolle entstehen, welche beinahe lückenlos Auskunft über das Leben einer Person geben, scheint jedenfalls

¹³ Roßnagel, Alexander / Müller, Jürgen (2004) *Ubiquitous Computing – neue Herausforderungen für den Datenschutz*. Computer und Recht, Heft 8/2004.

¹⁴ Roßnagel / Müller, a.a.O.

klar, dass man ohne effektive Maßnahmen zum Datenschutz eine feinmaschige Überwachungsinfrastruktur schaffen würde, welche viele bestehende Gesetze und Mechanismen zum Schutz der Privatsphäre aushebeln könnte.

Schon gibt es erste Produkte, z.B. in Form von Armbanduhren, mit denen man aus der Ferne den Aufenthaltsort seiner Kinder feststellen kann. Diese Armbanduhren sind noch nicht so bequem und energiesparsam, wie man es sich wünscht, aber die Technik macht ja Fortschritte! Nun mag ein 8-Jähriger das Tragen einer solchen Uhr „cool“ finden. Aber ist auch die 15-jährige Tochter bereit, sich damit auf Schritt und Tritt verfolgen zu lassen? Muss sie sich rechtfertigen, wenn sie die Fernlokalisierungsmöglichkeit einmal abschaltet? Sollte man nicht „vorsichtshalber“ auch entlassene Sträflinge verpflichten, so ein Gerät zu tragen? Oder – sollte die Technik zukünftig klein genug sein – Ausländern in das Visum integrieren („zum eigenen Schutz“)?

Im März 2004 berichtete „Bild.de“ folgendermaßen¹⁵ über einen neuen Lokalisierungsservice¹⁶ für Mobiltelefone: *Neuer Handy-Dienst sagt Ihnen immer, wo Ihr Kind ist. Ist es auch wirklich in der Schule? Mit „Track your kid“ finden Sie es heraus. Deutschlandweit können Sie so bis auf 250 m genau feststellen, wo sich der Nachwuchs aufhält. Das kann gerade für berufstätige Eltern oder Alleinerziehende eine Erleichterung sein. Denn diese sanfte Kontrolle verschafft Ihnen Sicherheit – und das Kind merkt gar nichts davon!*

Der seit November 2003 angebotenen Lokalisierungsdienst¹⁷ kostet 36 Euro Jahresbeitrag sowie 9,90 Euro Einrichtungsgebühr. Rechtlich ist daran nichts auszusetzen, da das Telekommunikationsgesetz die Weitergabe der Standortinformation zulässt, wenn der Handybesitzer dem zustimmt. Die ersten Reaktionen darauf waren unterschiedlich; im Diskussionsforum „Mama & Co“¹⁸ schrieb „happyanja“ zum Beispiel: *„Würde natürlich nicht alle zwei Stunden überprüfen. Nur, wenn ich mir mal Sorgen mache. Und ich würde ihn darüber informieren. Nicht, dass er sich ausspioniert vorkommt.“* Eine andere Teilnehmerin („Robse“) hatte mit ihrer Frage wohl eher einen anderen Einsatzzweck im Sinn und schrieb in ihrem Beitrag das Wort „man(n)“ vielleicht absichtlich und mit Hintersinn mit Doppel-n: *„Kann man das auch bei seinem Ehepartner anwenden? Nur mal so interessehalber.“* Im Deutschen Bundestag kam es u.a. deswegen im Mai 2004 zu einer Großen Anfrage¹⁹ der FDP-Fraktion: *„Wie beurteilt die Bundesregierung aus datenschutzrechtlicher Sicht Angebote GPS-basierter Handydienste wie Track your kid...? Sieht die Bundesregierung die informationelle Selbstbe-*

¹⁵ www.bild.t-online.de/BTO/handyc/toptemen/track__your__kid/trackyourkid.html

¹⁶ www.trackyourkid.de

¹⁷ Laut Meldung von „Spiegel Online“ vom Oktober 2004 hat der Dienst 7000 Kunden

¹⁸ www.gofeminin.de

¹⁹ Deutscher Bundestag (2004) *Überprüfung der personengebundenen datenschutzrechtlichen Bestimmungen*. Drucksache 15/3256.

stimmung von Kindern und Jugendlichen durch derart lokalisierbare Handys gefährdet...?“

Der Korrektheit wegen sei hier angemerkt, dass „Track your kid“ nicht, wie in der Anfrage suggeriert, das satellitengestützte GPS-System verwendet. Diese Möglichkeit dürfte erst ab etwa 2006 in handelsübliche Handys eingebaut werden, denn derzeit verbrauchen GPS-Empfänger dafür noch zu viel Strom und benötigen für genauere Messungen zu lange. Statt dessen wird ausgenutzt, dass im GSM-Mobilfunksystem die Funkzelle bekannt ist, in der sich ein Handy aufhält. Zwar ist die Funkzellendichte nur in Agglomerationsbereichen ausreichend hoch (einige wenige 100 Meter) und beträgt im ländlichen Raum bis zu 35 km, allerdings kennt die Basisstation einer Funkzelle die Entfernung der Handys zur Sendeantenne mit einer Granularität von etwa 550 m. Dies ist aus technischen Gründen (Synchronisation) notwendig und wird durch Laufzeitmessungen des Funksignals ermittelt. Befindet sich ein Handy im Überlappungsbereich mehrerer Funkzellen, dann kann im Prinzip durch Messung der Laufzeitunterschiede die Position auf etwa 300 m genau ermittelt werden. Bei UMTS, dem Mobilfunksystem der nächsten Generation, das zur Zeit eingeführt wird, wäre in technischer Hinsicht sogar eine Lokalisierung mit einer Genauigkeit von bis zu etwa 30 m möglich.

Je genauer und einfacher der Ort eines Handys oder eines anderen (kleinen, preiswerten) Gerätes ermittelt werden kann, umso vielfältiger und interessanter sind natürlich die möglichen Anwendungen. Andererseits wächst dadurch die Missbrauchsgefahr und erst langsam wird der Öffentlichkeit bewusst, dass die „location privacy“ ein Aspekt ist, um den man eventuell besorgt sein sollte.

Der Schutz der Privatsphäre ist ein Grundrecht – in der „Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen“ heißt es in Artikel 12: „Niemand darf willkürlichen Eingriffen in sein Privatleben... ausgesetzt werden“. Ähnlich ist es auch in der 1950 vom Europarat erarbeiteten „Europäischen Konvention für Menschenrechte und Grundfreiheiten“ formuliert (Artikel 8): „Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens...“. Dies hat für die Bürger der Ratifikationsstaaten insofern einen höheren Stellenwert als die Menschenrechtserklärung der Vereinten Nationen, als sie sich damit nach letztinstanzlichen Entscheidungen ihrer Behörden an den vom Europarat eingesetzten Europäischen Gerichtshof wenden können. Der Datenschutz als konkrete Ausprägung des Rechtes auf Privatheit wurde gesetzlich ebenfalls sehr grundlegend verankert – in Deutschland z.B. 1983 mit einem Leitspruch des Bundesverfassungsgerichts, das die informationelle Selbstbestimmung dem Persönlichkeitsrecht zuordnet, und in der Schweiz durch die Bundesverfassung von 1999, wo es bei den Grundrechten in Art. 13, welcher die Privatsphäre schützt, in Abs. 2 konkret heißt: „Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten“. International haben die OECD 1980, der Europarat 1981 und die Vereinten

Nationen 1990 in wichtigen Dokumenten ihre Mitgliedsstaaten angehalten, Datenschutzgesetze zu erlassen, im Jahr 2000 wurde der Schutz personenbezogener Daten schließlich in die Charta der Grundrechte der Europäischen Union aufgenommen.

Der Schutz der Privatsphäre und personenbezogener Daten ist aus gutem Grund so prominent aufgehängt. Denn hat man keine Privatsphäre, steht man leicht unter Druck von außen – das Wissen, dass Außenstehende jederzeit über Daten hinsichtlich der persönlichen Situation verfügen können, wirkt auf das eigene Verhalten zurück: Wer davon überzeugt ist, dass Fremde Daten über seine Verhaltensweise speichern oder weitergeben, wird sein eigenes Benehmen ändern und von seinen grundrechtlich verbrieften Freiheitsrechten nicht mehr in dem Maße Gebrauch machen, wie ihm dies die Verfassung eigentlich garantiert.²⁰ Es entspricht auch nicht der Würde des Menschen, wenn dieser nicht frei und selbstbestimmt entscheiden und handeln kann – und zur Würde heißt es schließlich schon in der Präambel der Menschenrechtserklärung, dass ihre Anerkennung die Grundlage der Freiheit, der Gerechtigkeit und des Friedens in der Welt bildet.

Der Stellenwert, welcher der Privacy im menschlichen Zusammenleben zukommt, kann man daran erkennen, dass ein schließlich aufgedeckter Missbrauch oft zu erheblichen, kaum reversiblen Vertrauensschädigungen führt. Lange Zeit gab es in der menschlichen Gesellschaft bezüglich der Privatsphäre einige Grundeigenschaften, die nur selten und schwer (durch Spione, heimliches Beobachten, explizite Täuschung) zu verletzen waren: Wenn der andere mich sieht, dann sehe ich ihn auch; wenn ich alleine bin, dann habe ich meine Privatsphäre; Personen, die mir fremd sind, kennen mich normalerweise auch nicht und wissen nichts oder wenig über mich. Diese traditionellen Erwartungen an die Privatsphäre werden durch die Telekommunikation und durch kleinste, fast unsichtbare Sensoren sowie die Möglichkeiten der Datenspeicherung nun aber außer Kraft gesetzt. Können wir uns als Gesellschaft so plötzlich daran gewöhnen, dass dies alles nicht mehr gilt? Die Ursache für die Probleme mit dem Privatsphärenschutz liegt jedenfalls unmittelbar im technischen Fortschritt selbst begründet: War früher die Verarbeitung von Daten stark durch die Schranken des Ortes und der Zeit, aber auch durch die Menge der Informationen eingengt, so sind diese Begrenzungen mit dem Internet weitgehend entfallen.²¹

Mit dem Einzug in das Zeitalter des ubiquitous computing und seiner Vision vom „Internet der Dinge“ verschärft sich die Situation noch: Billige und miniaturisierte Sensoren lassen sich massenhaft und fast überall anbringen; weil diese so klein sind, werden sie kaum mehr wahrgenommen; und weil die

²⁰ Garstka, Hansjürgen (2003) *Informationelle Selbstbestimmung und Datenschutz – Das Recht auf Privatsphäre*. In: Schulzki-Haddouti, Christiane (Hg.), *Bürgerrechte im Netz*. Bundeszentrale für politische Bildung, Schriftenreihe Bd. 382, 48–70.

²¹ Garstka, a.a.O.

Einzelbeobachtungen über Funk verbreitet werden, kann ein umfassendes Bild entstehen. Eine solche nahezu unsichtbare aber allgegenwärtige Technik zieht notgedrungen massive gesellschaftliche Probleme nach sich: Es könnte damit die delicate Balance von Freiheit und Sicherheit aus dem Gleichgewicht gebracht werden, weil die qualitativen und quantitativen Möglichkeiten zur Überwachung derart ausgeweitet werden, dass auch Bereiche erfasst werden, die einem dauerhaften und unauffälligen Monitoring bisher nicht zugänglich waren.

Rainer Kuhlen²² beobachtet einen anderen interessanten Trend: Im Zeitalter von E-Commerce und personalisierten Dienstleistungen wird Privatheit zunehmend nicht mehr als absolute Voraussetzung für ein selbstbestimmtes Leben angesehen, sondern wird zu einem aushandelbaren und partiell aufgebaren Gut. Sind genügend materielle Anreizangebote (z.B. Rabatte durch Kundenkarten, Preisnachlässe bei Autoversicherungen mit direktem Einblick auf die Fahrweise des Autos) oder Komfortvorteile vorhanden, so sind immer mehr Personen bereit, freiwillig auf ihre Privatheitsrechte zu verzichten. Offenbar wird von vielen, vielleicht sogar einer Mehrheit der Bevölkerung, eine Einschränkung der Privatheit nicht als gravierend empfunden. Nun mag man einwenden, dass dies kein grundsätzlich neuer Aspekt ist: Wollte man an der Museumskasse in den Genuss eines Seniorenrabatts kommen, so musste man sich schon immer mit seinem Alter outen. Auch hier sind es aber wieder die durch den Technikfortschritt ermöglichte quantitative Zunahme und der Aspekt der Globalisierung durch totale Vernetzung²³, die dem Ganzen eine neue Qualität verleihen.

Beate Rössler²⁴ sieht selbst die freiwillige Beschränkung informationeller Privatheitsrechte problematisch, und zwar in Hinblick auf die Demokratie, weil *„die freiwillige wie die unfreiwillige Verminderung des Schutzes informationeller Privatheit dazu führen kann, dass bestimmte Formen und Dimensionen selbstbestimmten und authentischen Verhaltens... als weniger relevant... für ein gelungenes Leben begriffen werden. Das hieße dann nämlich auch, dass das Selbstverständnis von Personen sich ändert, wenn und insofern sie in wichtigen Hinsichten ihres Lebens darauf verzichten, unbeobachtet, unidentifizierbar, nicht zugänglich zu sein. Dies trifft dann jedoch... auch die Idee der liberalen Demokratie, die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist.“*

²² Kuhlen, Rainer (2004) *Informationsethik. Ethik in elektronischen Räumen (Kapitel 6: Privacy in elektronischen Räumen – informationelle Selbstbestimmung, informationelle Autonomie)*. UTB.

²³ Mattern, Friedemann (Hg.) (2003) *Total vernetzt – Szenarien einer informatisierten Welt*. Springer-Verlag.

²⁴ Rössler, Beate (2003) *Der Wert des Privaten*. In: Grötter, Ralf. (Hg), *Privat! Kontrollierte Freiheit in einer vernetzten Welt*. Heise, 15–32.

Durch den technischen Fortschritt bedingt wandelt sich hinsichtlich des Bedrohungspotentials der Privatsphäre noch ein anderer Aspekt: Während man in den Anfangszeiten des Datenschutzes zunächst den allwissenden Staat beargwöhnte, inzwischen aber mehr und mehr informationshungrige Marketingabteilungen großer Firmen im Blickfeld hat, werden mit Foto-Handy, GPS-Lokalisatoren und in die Kleidung integrierten Sensoren und Computern einzelne Personen (oder sogar smarte Gegenstände, für die sich niemand mehr richtig verantwortlich fühlt) zu Datensammlern. An die Stelle des einen allwissenden „großen Bruders“ könnten zahllose „kleine Geschwister“ in Form neugieriger Nachbarn und eifersüchtiger Bekannter treten, deren Hemmschwelle für ein gelegentliches Bespitzeln mit dem technischen Aufwand für solch eine Überwachung sinken dürfte.

Eine solche Entwicklung stellt natürlich eine Herausforderung an Recht und Politik dar. Roßnagel, Pfitzmann und Garstka haben 2001 erstmalig das Potential der allgegenwärtigen Informationstechnik im juristischen Kontext thematisiert und halten die Problematik in ihrem Gutachten *Modernisierung des Datenschutzrechts*²⁵ fest, indem sie schreiben: „Künftig ist jedoch zu erwarten, dass der Einzelne nicht nur Datenspuren seiner Handlungen in der für ihn abgegrenzten Welt des Cyberspace hinterlässt, sondern auch durch vielfältigste Handlungen in der realen Welt. Weitere Leistungssteigerungen der Informations- und Kommunikationstechnik, kleinste Sensoren und Akteure sowie neue Materialien zur Darstellung von Daten werden dazu führen, dass tendenziell jeder Gegenstand Rechenkapazität erhält und kommunikationsfähig wird. Diese Ubiquität der Datenverarbeitung und das Verschwinden des Computers werden eine neue Qualität personenbezogener Datenverarbeitung bringen.“ Weiter heißt es dort: „Datenverarbeitungskapazität wird in Alltagsgegenstände eingebaut sein – in der Brille, im Ohrring, in der Kaffeemaschine, in der Heizung, im Auto, im Koffer oder in jedem Verkaufsgegenstand im Kaufhaus, sogar in intelligentem Staub. Durch kontaktlose Datenübertragung kann das Auto seinen Besitzer erkennen, die Heizung den Hausbewohner, der Ohrring den Gesprächspartner, sich auf den jeweiligen Berechtigten einstellen oder diesen an ein bestimmtes Gesprächsthema erinnern.“ Und weiter: „Niemand wird mehr im Voraus wissen können, welche Daten von diesen Gegenständen erhoben und zwischen ihnen kommuniziert werden. Auf diese Entwicklung allgegenwärtiger Datenverarbeitung ist das Datenschutzrecht noch überhaupt nicht vorbereitet.“

Es sind neben intensiven technischen und organisatorischen Anstrengungen auf den Gebieten Sicherheit und Datenschutz daher auch grundlegende rechtliche Maßnahmen nötig, um die schöne neue Welt voller aufmerksamer und kommunikationsfreudiger Dinge nicht in einen orwellschen Überwa-

²⁵ Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen (2001) *Modernisierung des Datenschutzrechts*. Bundesministerium des Inneren, Berlin.

chungsstaat zu verwandeln. In ihrem Aufsatz „*Ubiquitous Computing – neue Herausforderungen für den Datenschutz*“²⁶ greifen Roßnagel und Müller die rechtliche Dimension unter der Prämisse auf, dass auch in einer Welt des ubiquitous computing das Grundrecht auf informationelle Selbstbestimmung gelten muss, sofern diese Welt human und lebenswert sein soll. Sie analysieren dabei, inwiefern durch die absehbare technische Entwicklung das normative Schutzprogramm des derzeitigen deutschen Datenschutzrechts in Frage gestellt wird. Zu diesem gehören traditionell *Transparenz* (der Betroffene weiß, wer was wann über ihn weiß bzw. erfährt), *Einwilligung* (als eigentlicher Ausdruck der informationellen Selbstbestimmung), *Zweckbindung* (und damit einhergehend eine Zweckbegrenzung), *Erforderlichkeit* (inklusive Minimierung und frühzeitiges Löschen personenbezogener Daten), sowie *Auskunfts-* und *Korrekturrecht*.

Bezüglich aller genannter Aspekte kommen die Autoren zum Schluss, dass diese in einer Welt des ubiquitous computing kaum in der bisherigen Weise garantiert werden können. Hinsichtlich der Transparenz würden es die Betroffenen beispielsweise nicht akzeptieren, täglich zigfach Hinweise über ansonsten im Hintergrund ablaufende Datenerhebungsvorgänge zur Kenntnis zu nehmen. Auch die explizite Einwilligung würde an Fülle und Vielfalt der Vorgänge und beteiligten Stellen scheitern. Den Zielen der Zweckbindung und Erforderlichkeit widerspricht die Idee, viele Daten auf Vorrat für einen nur möglichen, im Detail unbekanntem späteren Nutzen zu sammeln, um so ein „smartes“, also z.B. auf Erfahrung beruhendes, Verhalten zu ermöglichen oder auch nur dem Nutzer eine Erinnerungsfunktion für zukünftige Zwecke zu bieten. Schließlich könnte das Auskunfts- und Korrekturrecht daran scheitern, dass unklar ist, welche automatisch gewonnenen Daten überhaupt verarbeitet werden; darüber hinaus dürfte für viele Anwendungen zum Zeitpunkt der Datenerhebung noch nicht feststehen, ob die Daten überhaupt personenbezogen sind, da sie einen möglichen Personenbezug vielfach erst später erhalten.

Ergänzend dazu sei noch bemerkt, dass auch der in letzter Zeit verstärkt in die Datenschutzdiskussion eingebrachte Aspekt der „Zurechenbarkeit“²⁷ Probleme bereiten dürfte. Darunter versteht man die Forderung, dass von jeder in einem IT-System ausgeführten Aktion während ihres Ablaufs und danach feststehen muss, wem diese Aktion zuzuordnen ist und wer sie letztlich zu verantworten hat. 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 smarte Alltags-

²⁶ Roßnagel / Müller, a.a.O.

²⁷ Dierstein, Rüdiger (2004) *Sicherheit in der Informationstechnik – der Begriff der IT-Sicherheit*. Informatik-Spektrum 27(4), 343–353.

dinge gewissermaßen selbst nicht genau wissen, wieso sie bezogen auf den konkreten Kontext ein spezifisches Verhalten aufweisen, ein schwieriges Unterfangen. Zu einem Vorgang 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. Diese Problematik der *Dissipation der Verantwortung*, aber auch damit verbundene Haftungsfragen (z.B.: bin ich als Besitzer oder ist der Hersteller für die Handlungen eines smarten, autonom agierenden Objektes verantwortlich?), dürfte mit dem ubiquitous computing stark an Bedeutung gewinnen und bedarf in Zukunft vielleicht sogar einer eigenständigen Regelung.

Roßnagel und Müller kommen in ihrem Aufsatz jedenfalls zum Schluss, dass bedingt durch den Paradigmenwechsel in der Datenverarbeitung neue normative Ansätze im Datenschutz implementiert werden müssen. Hierzu gehören effektive Kontrollstellen, die das Vertrauen der Betroffenen genießen und stellvertretend für diese arbeiten, Ansätze bei der Technikgestaltung sowie die Anwendung von Vorsorgeprinzipien hinsichtlich Daten, die später einmal mit einem Personenbezug versehen werden könnten. Bezüglich ergänzender und prinzipiell neuer Maßnahmen im Datenschutzrecht, die den Bedingungen des ubiquitous computing gerecht werden, stehen wir aber sicherlich erst am Anfang einer längeren Diskussion.

Dass wir im Zuge der „digitalen Globalisierung“ überhaupt größere Probleme mit der Privatsphäre bekommen, hat eine tiefere und gleichzeitig pauschale Ursache, die auch für anderer Verwerfungen ursächlich ist: Die „Defaults“ kehren sich in vielen Fällen um, wie es Ronald Rivest im Informatik-Fachjargon einmal ausgedrückt hat – was heißen soll, dass die Standardannahmen auf den Kopf gestellt werden: was früher ein Spezialfall oder eine Ausnahme war, wird zum Normalfall und umgekehrt. Rivest, übrigens einer der drei Erfinder des berühmten RSA-Verschlüsselungsverfahrens, führte dies in plakativer Weise so aus: „*What was once private is now public. What was once hard to copy is now trivial to duplicate. What was once forgotten is now stored forever.*“ Und tatsächlich: Musste man früher viel Geld, Zeit und Energie aufwenden, um Information zu verbreiten, so muss man heute, wie es die Musik- und Filmindustrie gelernt hat, viel Geld, Zeit und Energie aufwenden, damit etwas *nicht* vervielfältigt wird. Und musste man früher Pyramiden bauen, um unvergessen zu bleiben, so kann man heute Jugendsünden, die man ins Internet geschrieben hat, auch mit viel Aufwand kaum mehr loswerden – Suchmaschinen spüren diese auch Jahrzehnte später noch auf, selbst dann, wenn man die Originalquellen beseitigt hat!

D.III Dinge mit Gedächtnis

Speicher wird immer billiger, und die Speicherkapazitäten nehmen rasant zu. Dadurch wird kaum noch etwas endgültig gelöscht (also „vergessen“), und das im Internet Gespeicherte kann fast immer schnell und mit wenig Aufwand wieder gefunden werden. Schon heute stellt dies für manche ein Problem dar, die deswegen abträgliche Aspekte aus ihrer Vergangenheit nicht loswerden oder falschen Tatsachen, die über sie verbreitet wurden, nicht effektiv entgegenreten können. Sogar die modernen Telekommunikationsnetze und -dienste selbst haben, im Unterschied zum klassischen „Fernmeldenetz“ und teilweise aus nachvollziehbaren technischen oder organisatorischen Gründen, ein Erinnerungsvermögen; ihre Nutzung hinterlässt daher Spuren.

Der Speicheraspekt gewinnt im ubiquitous computing aber noch an Dramatik. Denn jetzt bekommen auch immer mehr Alltagsdinge ein Gedächtnis – meistens damit wir Nutzer es leichter haben, manchmal aber auch, damit Hersteller ihre Produkte auch noch kontrollieren können, wenn diese bei den Kunden eingesetzt werden: Telefone speichern die Nummern aller Anrufer und Angerufenen, Autos den Zeitpunkt des letzten Ölwechsels, Kaffeemaschinen die Zahl der zubereiteten Tassen Kaffee (damit die Garantie bei heftigem Gebrauch auch rechtzeitig erlöschen kann), LCD-Projektoren ihre Betriebszeiten (damit Kunden früh genug gezwungen werden, eine Ersatzlampe zu kaufen), und DVD-Player auf Laptop-Computern den Namen des jüngst abgespielten Films. Letzteres ist ein nettes „feature“, kann aber auch zum Verhängnis werden, wenn etwa ein Lehrer seiner Schulklasse ein Video zeigen möchte, der Player vorher aber allen Zuschauern den Namen des nicht jugendfreien Films verrät, den dieser sich am Abend vorher angesehen hat. Zwar bieten PC-Betriebssysteme und einige Anwendungen (wie z.B. der Internet Explorer, der sich die zuletzt besuchten Web-Seiten merkt) im Allgemeinen eine Möglichkeit, die sogenannte „History-Liste“ der zuletzt betrachteten Dokumente oder zuletzt durchgeführten Aktionen zu löschen, dies ist aber typischerweise mit einem Verlust an Komfort verbunden und wird, da es dazu einer expliziten Aktion bedarf, oft vergessen oder vernachlässigt. Einer auch nur amateurhaft durchgeführten „forensischen“ Analyse des PCs hält dieses Löschen der History-Liste sowieso nicht stand, da Spuren vergangener Aktivitäten sich an verschiedenen Stellen („Registry“, Temporärdateien etc.) im System finden.

Legendär sind auch die Beziehungsdramen, die sich dadurch ergeben, dass Telefone verraten, mit wem, wann und wie lange telefoniert wurde, oder dass sich jemand in einem anderen Land als angegeben aufhält. (*Liebesfalle Handy* lautete die Titelgeschichte eines Nachrichtenmagazins dazu kürzlich.) Smarte Dinge verletzen also leicht die Privatsphäre, indem sie etwas ausplaudern, was nicht für andere bestimmt war. Da in Zukunft immer mehr Dinge informatisiert werden (zum Beispiel Schreibstifte, die alles digitalisieren, was mit

ihnen geschrieben wird) und auch ein Ortsbewusstsein bekommen können (zum Beispiel Reisetaschen, die ihrem Besitzer mitteilen, wo sie „gestrandet“ sind und sich an besuchte Orte zu erinnern vermögen), darf man sich hier noch auf einiges gefasst machen!

Das Beispiel der ortsbewussten Reisetasche zeigt auch ein grundsätzliches definitorisches Problem auf: Was sind denn genau „personenbezogene“ Daten, die in rechtlicher Hinsicht herausgehoben sind, da sie einem besonderen Schutz unterliegen? Bei den Orten, die eine Reisetasche besucht hat, handelt es sich zunächst um harmlose Daten; eine datenschutzrelevante Bedeutung erlangen diese ja erst (nachträglich?), wenn bekannt wird, dass es sich um „meine“ Tasche handelt! Auch erscheint, wie oben bereits angedeutet, die bisher durch den Gesetzgeber erhobene Forderung nach prinzipieller Zweckgebundenheit aller gewonnenen (personenbezogenen) Daten in einer Zukunft voll schlauer Alltagsdinge kaum mehr adäquat, da sie das Gedächtnis solcher Gegenstände so gut wie verbietet – der wesentliche Vorteil eines Artefakt-Gedächtnisses liegt aber gerade in der Speicherung von Information für zukünftige, jedoch a priori unbekannt Zwecke. Da bei einer strikten Auslegung von Datenschutzgesetzen (die vielfach zu einem Zeitpunkt entstanden sind, als die hier skizzierten technischen Möglichkeiten noch unbekannt waren) viele nette neue Anwendungen, die beispielsweise die nachträgliche Rekonstruktion des Ortsbezugs oder ein episodisches Gegenstandsgedächtnis voraussetzen, unmöglich würden, darf man gespannt sein, wie sich die gesellschaftliche und gesetzgeberische Diskussion hier weiterentwickelt.

Generell birgt die sekundäre Nutzung von Daten jenseits ihres ursprünglichen Zwecks allerdings einiges an Konfliktpotential. An die Stelle eines öffentlichen Aufrufs an potentielle Zeugen nach einem Verbrechen könnte in Zukunft beispielsweise die freiwillige Freigabe der persönlichen sensorischen Datenbanken treten. Ähnlich den immer populärer werdenden freiwilligen DNA-Analysen würden sich bei solchen Maßnahmen all jene verdächtig machen, die den Sicherheitsorganen den uneingeschränkten Zugriff auf das digitale Gedächtnis ihrer Dinge verweigern.

Eher philosophisch betrachtet stellt sich in diesem Kontext die Frage, ob wir nicht ein Recht auf Vergessen haben sollten. Hängt das Vergessen nicht auch mit dem Verzeihen zusammen („Zeit heilt alle Wunden“)? Wäre es nicht unmenschlich, wenn jede kleine Verfehlung einem immer wieder vorgehalten werden kann? Wäre das nicht letztlich sogar gegen die menschliche Würde? Im Recht gibt es immerhin das Prinzip der Verjährung – man darf dabei wohl davon ausgehen, dass dies nicht nur deswegen Bestand hat, weil nach langer Zeit Zeugenaussagen undeutlich werden und Beweiskontexte verschwimmen, sondern dass dabei auch die „Gnade der Zeit“ eine Rolle spielt.

Das Vergessen scheint eine natürliche menschliche Eigenschaft zu sein – so natürlich, dass man offenbar nicht daran gedacht hat, es explizit als Menschenrecht zu formulieren (und wohl auch einfach deswegen, weil man ohne-

hin nicht erzwingen kann, dass ein Mensch etwas vergisst). Wenn aber nun Dinge *aufmerksam* werden und informationstechnische Systeme alles „auf ewige Zeit“ abspeichern – müssen wir dann dieses implizite Recht nicht explizit einfordern?

Bruno Glaus geht in seinem jüngst verfassten Aufsatz „Das Recht auf Vergessen und das Recht auf korrekte Erinnerung“²⁸ auf diesen Aspekt unter juristischen Gesichtspunkten ein und ruft in Erinnerung, dass das schweizerische Bundesgericht schon 1983 (in einer allerdings umstrittenen Entscheidung zu einer konkreten Klage wegen Verletzung der Persönlichkeitsrechte) ein „Recht auf Vergessen“ postuliert und im Oktober 2003 bestätigt hat.²⁹ Das Gericht stellte seinerzeit fest, dass das mit dem Strafvollzug verknüpfte Ziel der Resozialisierung verlange, „dass das dem normalen Lauf der Dinge entsprechende Vergessen eintreten kann“³⁰. Auch wenn besonders Interessierte sich immer erinnern können, rechtfertige dies nach Meinung des Gerichts nicht, dass die Vergangenheit erneut in das Bewusstsein der Öffentlichkeit gebracht werde. (Insofern ist, wie Glaus mit dem Zitat einer Anmerkung von Christian Brückner³¹ bemerkt, der Begriff des „Rechts auf Vergessen“ zwar einprägsam, aber unpräzise. Es gehe genauer um die Unterlassung des öffentlichen In-Erinnerung-Rufens.)

Medienrechtlich hat dies natürlich Konsequenzen, etwa bei der Frage, ob eine gelöschte Vorstrafe veröffentlicht werden darf. Zwar ist das Problem, inwieweit im Einzelfall die öffentliche Bekanntmachung von Archivmaterial mit dem Persönlichkeitsschutz in Konflikt steht, kein neuer Aspekt, doch gewinnt dies im Zeitalter des Internet an Bedeutung und Brisanz, vor allem wegen der leicht zugänglichen und durchsuchbaren Zeitungsarchive im Netz. Der Schweizer Presserat hat dazu im Jahr 2001 festgestellt, dass ein Medium berufsethisch verpflichtet sei, eine Gegendarstellung solange online durch Verlinkung zugänglich zu machen, als auch auf den Hauptartikel entsprechend zugegriffen werden kann.

Zweifellos kommt nun, im Zeitalter des ubiquitous computing, noch einiges mehr in Hinblick auf das unerwünschte Erinnern auf uns zu, wenn sogar ganz banale Alltagsdinge ein Gedächtnis bekommen und zu aufmerksamen, vernetzten und mitteilbaren Medien werden!

²⁸ Glaus, Bruno (2004) *Das Recht auf Vergessen und das Recht auf korrekte Erinnerung*. Zur Veröffentlichung eingereicht.

²⁹ Schweizerisches Bundesgericht (2003) BGE-Entscheid 5C.156/2003.

³⁰ Schweizerisches Bundesgericht (1983) BGE-Referenz 109 II 353.

³¹ Brückner, Christian (2000) *Das Personenrecht des ZGB*. Schulthess, Rz 498 ff (zitiert nach Bruno Glaus).

D.IV Ethische Fragestellungen

Die globale Informatisierung hat über die oben betrachteten Aspekte hinaus noch einige weitere potentielle Auswirkungen, die kritisch hinterfragt werden müssen. So könnte es etwa vermehrt dazu kommen, dass die Unschuldsvermutung nicht mehr a priori angenommen wird und nicht die Schuld bewiesen werden muss, sondern man seine Unschuld nachweisen muss. („Wenn der Angeklagte nichts zu verbergen hat, dann hätte er doch nicht gerade im kritischen Moment seinen aus der Ferne lokalisierbaren Identifikator abgeschaltet.“) Die tiefere Ursache liegt auch hier wieder darin, dass durch die generelle Digitalisierung und die Globalisierung des Informationsaustausches einige Grundannahmen fast auf den Kopf gestellt werden. Mit der Unschuldsvermutung sollte allerdings nicht leichtfertig umgegangen werden, sie ist immerhin ein Grundrecht: *Jeder Mensch... ist so lange als unschuldig anzusehen, bis seine Schuld... nachgewiesen ist* (Allgemeine Erklärung der Menschenrechte, Artikel 11).

Menschen wollen gleich und fair behandelt werden. Auch dazu finden sich in der Allgemeine Erklärung der Menschenrechte einige Hinweise. Etwa, dass alle Menschen die gleichen Rechte haben sollen (Präambel) oder dass man für die gleiche Arbeit den gleichen Lohn erhalten soll (Artikel 23). Durch die Möglichkeit, exakte Kundenprofile zu erstellen, was durch die neue Technik stark erleichtert wird, kann man nun aber in vielen Fällen individuelle Preise für Dienstleistungen oder gar Produkte festsetzen – und so im Extremfall von einem Kunden gerade so viel verlangen, wie dieser noch bereit ist zu bezahlen.³² Ist eine solche Preisdiskriminierung volkswirtschaftlich oder im Sinne einer Markttheorie zweckmäßig? Oder unmoralisch und unfair? Verstößt dies gegen das Gleichheitsgebot? Oder wird so etwas in der Praxis dann derart subtil gemacht, dass sich gar niemand benachteiligt fühlt?

Weitere potentielle Problembereiche, die durch die Verlängerung des Internets in die Alltagswelt hinein entstehen, seien hier nur noch angedeutet: Wenn beispielsweise vernetzte und „elektronisch aufgewertete“ Alltagsdinge Information von sich geben, physische Dinge also quasi zu Medien ihrer selbst werden, dann stellt sich die Frage, wer über den Inhalt bestimmen darf und wer die Objektivität und Richtigkeit von „Aussagen“ smarter Produkte garantiert. Wer legt beispielsweise fest, was eine smarte Sprechpuppe den Kindern erzählt? (Darf sie um das neue Kleidchen aus der Fernsehwerbung betteln?) Oder darf eine Verbraucherschutzinstitution die in einem elektronischen Etikett eines Fertiggerichtes gespeicherte Identifikationsnummer auf eine andere Information umlenken, als es der Hersteller vorgesehen hat, um so beispielsweise vor Allergenen bei den Inhaltsstoffen zu warnen?

³² Odlyzko, Andrew (2003) *Privacy, Economics, and Price Discrimination on the Internet*. www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf.

Die technischen Möglichkeiten des ubiquitous computing könnten im Einzelfall auch bewirken, dass die Meinungsfreiheit eingeschränkt wird, selbstbestimmtes Handeln erschwert wird und es zu Kontrollverlusten kommen kann – unter anderem deswegen, weil vieles minutiös aufgezeichnet und aufbewahrt wird und man sich dadurch kontrolliert und unfrei fühlen kann, oder weil immer mehr Prozesse autonom ablaufen, Dinge einen eigenen Willen bekommen und die automatisierten Vorgänge nicht mehr im Detail nachvollziehbar sind (vgl. auch Bohn et al.³³). Erst die Zukunft wird zeigen, ob hier tatsächlich ein ernstes Problem entstehen kann und gegengesteuert werden muss.

E. Fazit

Bei all den kritischen Betrachtung des letzten Kapitels sollte man jedoch die vielen Vorteile, welche die fortschreitende Informatisierung des Alltags haben kann, nicht vergessen: Man hat unmittelbar Zugriff auf vielfältige Informationsquellen, man kann Information relativ einfach bereitstellen statt sie nur zu konsumieren und chronisch kranke Personen oder ältere Leute können vielfach ein selbstbestimmteres Leben führen, da sie dank der Technik weniger oft auf die direkte Hilfe anderer Menschen angewiesen sind. Und ganz allgemein wird das Leben – zumindest vordergründig – in mancher Hinsicht einfacher und angenehmer.

Was erwartet uns also? Dürfen wir optimistisch in die Zukunft blicken? Oder müssen wir uns Sorgen machen? Klar ist: Technik und Wissenschaft haben generell einen großen Einfluss auf die Gesellschaft und unsere Welt. Die Beispiele „Automobil“ oder „Rundfunk“ zeigen, dass die wesentliche Wirkung oft aber erst Generationen später einsetzt und sich damit kaum vorhersehen oder gar im Vorhinein bewerten lässt.

Bei der exponentiellen Leistungszunahme der Mikroelektronik und Digitaltechnik handelt es sich um eine „schleichende Revolution“ – sie ist die ganze Zeit im Gange und wird dadurch kaum wahrgenommen. Ihr Effekt ist jedoch nicht direkt proportional zur Leistungszunahme: Wenn eine gewisse kritische Masse an „Innovationspotential“ vorhanden ist, kann eine Wirkung sehr schnell entfaltet werden – ein Beispiel hierfür war etwa die Nutzung des Mobiltelefons. Ein Problem bei diesem Prozess stellt die Tatsache dar, dass die soziale Anpassung an umfassende Änderungen der Lebensumstände Zeit benötigt – oft ist erst die nachfolgende Generation dazu bereit. Gelingt uns dies aber bei der rasanten digitalen Revolution? Bleibt uns dafür genügend

³³ Bohn, Jürgen / Coroama, Vlad / Langheinrich, Marc / Mattern, Friedemann / Rohs, Michael (2004) *Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications*. *Journal of Human and Ecological Risk Assessment* 10(5), 763–786.

Zeit? Oder tun sich dann vielleicht zwischen Jung und Alt doch „digitale Gräben“ auf?

Jedenfalls dürfte die allgegenwärtig und allumfassend werdende Informationstechnik interessante Konsequenzen haben – und zwar in wirtschaftlicher Hinsicht, aber auch in Hinblick auf die Gesellschaft allgemein und deren Kultur. Eine der wichtigsten Herausforderungen wird dabei sein, unsere sozialen Werte und Grundrechte wie den Schutz der Privatsphäre, die Meinungsvielfalt oder das selbstbestimmte Handeln nicht zu gefährden und so die menschliche Würde auch in einer Welt smarterer Alltagsdinge zu erhalten.

Die Informatik hat es mit dem Internet geschafft, alle Rechner und PCs der Welt, immerhin mehrere 100 Millionen an der Zahl, zu vernetzen. Ohne sich dessen so richtig bewusst zu werden, beginnt man nun, in die reale Welt einzugreifen, indem man deren Gegenstände informatisiert und zu einem „Internet der Dinge“ vernetzt. Wir leben zweifellos in interessanten Zeiten, und man darf auf die Zukunft gespannt sein!