Literatur

Bitkom – Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V., 2007: Mehrheit der Deutschen will elektronische Gesundheitskarte nutzen. Berlin; http://www.bitkom.org/48786_48781.aspx; download 20.03.2008

DÄT – Deutscher Ärztetag 2005: Bundesärztekammer (Hg.), 2005: Beschlussprotokoll des 108. Deutschen Ärztetages vom 3. - 6. Mai 2005 in Berlin, Berlin

DÄT – Deutscher Ärztetag 2007: Bundesärztekammer (Hg.), 2007: Beschlussprotokoll des 110. Deutschen Ärztetages vom 15.-18. Mai 2007 in Münster, Berlin

Dierks, C., 2005: Rechtliche Aspekte der Gesundheitstelematik. In: Bundesgesundheitsblatt 48 (2005), S. 635-639

Groß, C., 2006: Gesundheitstelematik: Folgen für die Arzt-Patient-Beziehung. In: Deutsches Ärzteblatt 103/51-52 (2006), S. A3469-A3471

Hornung, G., 2008 nach: Brenn, J.: Ärzte begleiten Telematikprojekt weiter skeptisch. In: Rheinisches Ärzteblatt 62/3 (2008), S. 10-12

SGB V 291: Sozialgesetzbuch V § 291 (Krankenversichertenkarte)

SGB V 291a: Sozialgesetzbuch V § 291a (Elektronische Gesundheitskarte)

SGB V 291b: Sozialgesetzbuch V § 291b (Gesellschaft für Telematik)

Stachwitz, P., 2007: Die elektronische Gesundheitskarte aus ärztlicher Sicht. In: Bales, S.; Dierks, C.; Holland, J.; Müller, J.H. (Hg.): Die elektronische Gesundheitskarte. Heidelberg, S. 343-347

Kontakt

Dr. med. Philipp Stachwitz
Stellv. Dezernent Telematik
Hauptgeschäftsführung
Bundesärztekammer
Herbert-Lewin-Platz 1, 10623 Berlin
E-Mail: philipp.stachwitz@baek.de
Internet: http://www.baek.de

« »

Datenschutz bei Pervasive Computing im Gesundheitswesen

von Johann Čas, ITA

Den versprochenen Vorteilen „allgegenwärtiger Informationstechnologien“ („pervasive computing“) stehen eine Reihe von Nachteilen gegenüber, die individuelle und gesellschaftliche Werte in Frage stellen und bestehende Eckpfeiler demokratischer Gesellschaften zu unterhöhlen drohen. Insbesondere zum Grundrecht auf Privatsphäre sind prinzipielle Konflikte und Widersprüche auf den ersten Blick erkennbar. Der Hauptteil dieses Beitrags ist der Analyse von Widersprüchen zwischen Systemen des Pervasive Computing und dem Datenschutz gewidmet. Daran schließt eine Diskussion der Besonderheiten an, die aus dem spezifischen Einsatzbereich Gesundheitswesen resultieren. Gesundheitsdaten stellen offensichtlich besonders sensible persönliche Daten dar, Gefährdungen der Gesundheit betreffen aber oftmals elementare, lebensbedrohende Ereignisse, die Eingriffe in Grundrechte eher gerechtfertigt erscheinen lassen.

Pervasive Computing steht als einer von vielen Begriffen für ein neues Paradigma der Informationstechnologie. Das Ziel dieser technologischen Entwicklung lässt sich als ein „Schlaraffenland“ der Informationen beschreiben: Die gewünschten Informationen fliegen den NutzerInnen förmlich zu, ohne künstliche Interfaces verwenden zu müssen; Befehle in natürlicher Sprache oder Gesten allein, vielleicht aber auch eine unbemerkte Analyse des Kontextes reichen aus, um Suchmaschinen in Gang zu setzen, welche in unaufdringlicher Weise ihre Resultate präsentieren oder einfach nur die Raumtemperatur oder Hintergrundmusik an die persönlichen Bedürfnisse anpassen. Um diesen Traum von TechnikerInnen Realität werden zu lassen, bedarf es einer unaufdringlichen und unbemerkten Durchdringung der Umwelt mit Informationstechnologien. Diese können in den eigenen Körper, die Kleidung, Alltagsgegenstände oder die Umgebung eingebettet sein. Offensichtlich eignen sich die Technologien des Pervasive Computing hervorragend, um eine perfekte Überwachungsinfrastruktur aufzubauen. Es herrscht zwischen den in diesem For-

schungsfeld tätigen WissenschaftlerInnen weitgehend Einigkeit, dass besondere Anstrengungen notwendig sein werden, damit diese technische Entwicklung nicht in einer Überwachungsgesellschaft mündet (Mattern, Langheinrich 2001).

Trotz der Anerkennung der Bedrohungen für die Privatsphäre, die vom Pervasive Computing ausgehen, und der zahlreichen Versuche, technische oder organisatorische Vorkehrungen zu treffen, um die Vorteile des Pervasive Computing ohne Einschränkungen des Grundrechts auf Privatsphäre genießen zu können, fehlt es an überzeugenden Konzepten zur Aufhebung der Widersprüche (Čas 2004). Dieses Manko ist aber nicht auf fehlendes Interesse, mangelndes Engagement oder Know-how zurückzuführen, sondern liegt in den prinzipiellen Widersprüchen zwischen der Vision von Pervasive Computing und den Säulen begründet, auf denen der Datenschutz aufbaut. Wie im nächsten Abschnitt näher ausgeführt wird, ist Pervasive Computing mit der Wahrung des Grundrechts auf Privatsphäre in wesentlichen Punkten unvereinbar.

Eine derart negative Einschätzung lässt für die Nutzung von Pervasive-Computing-Systemen im Gesundheitswesen auf den ersten Blick kaum eine positivere Beurteilung erwarten. Laut Art. 8 der Datenschutzrichtlinie (Europäisches Parlament und der Rat 1995) zählen Daten über die Gesundheit zu den besonderen Kategorien von Daten, deren Verarbeitung erst einmal generell untersagt ist. Eine der wenigen, aufgezählten Ausnahmen betrifft das Gesundheitswesen, wobei aber eigens auf das ärztliche Berufsgeheimnis oder entsprechende Geheimhaltungspflichten der mit der Verarbeitung betrauten Personen verwiesen wird. Systeme des Pervasive Computing im Gesundheitswesen müssen daher mit entsprechenden Vorkehrungen und Sicherheitsmaßnahmen ausgestattet sein, um dem geforderten, besonderen Schutzniveau zu entsprechen. Inwieweit sich die grundsätzlichen Widersprüche zwischen Pervasive Computing und Datenschutz im spezifischen Kontext des Gesundheitswesens auflösen lassen, und welche Auflagen zu diesem Zweck erfüllt sein müssen, wird in Abschnitt 2 skizziert.

Eine gründliche Diskussion der Begriffe „Gesundheit“ und „Krankheit“ würde den Rahmen dieses Beitrags bei weitem sprengen. Wenn es aber um die Abwägung von Eingriffen in die und Verletzungen der Privatsphäre einerseits mit Zugewinnen an Gesundheit andererseits geht, wird man sich dieser Begriffsdiskussion nicht ganz entziehen können. Gesundheit gilt zu Recht als ein individuell und gesellschaftlich sehr hoch bewertetes Gut. Krankheit ist mit Unwohlsein, Einschränkungen der Leistungsfähigkeit, Schmerz und Leid verbunden und kann letztlich den Verlust der Existenz bedeuten. ÄrztInnen bzw. Personen, die sich um die körperliche oder seelische Gesundheit kümmern, wird deshalb oft ein Vertrauen entgegengebracht, welches selbst ein Eindringen in tiefste Sphären der Intimität und in den eigenen Körpers erlaubt. Gerade dieses hohe Vertrauen, das dem Gesundheitssystem im Allgemeinen entgegengebracht wird, verlangt nach einer kritischen Analyse, wenn es um die Abwägung von Vor- und Nachteilen und um die Einführung, Förderung, Akzeptabilität und Akzeptanz neuer Technologien geht. Bei Anwendungen des Pervasive Computing im Gesundheits- und Pflegesektor erscheint eine nüchterne Betrachtung besonders dringlich, geht diese Technologie doch mit einem doppelten Heilsversprechen ins Rennen um die Gunst der Politik, der Anwender und der kranken oder pflegebedürftigen Personen. Das doppelte Heilsversprechen besteht darin, sowohl den betroffenen Patienten eine bessere und effizientere Behandlung oder Betreuung zukommen zu lassen, also auch das Gesundheitssystem selbst vor dem drohenden finanziellen Kollaps zu retten (Varshney 2003).

1 Widersprüche zum Rechtsgut ‚Schutz der Privatsphäre’

Die folgenden Ausführungen[1] beziehen sich auf die Vision des Ubiquitous oder Calm Computing von Mark Weiser im Sinne einer unaufdringlichen und unbemerkbaren Durchdringung von Alltagsgegenständen und der Umwelt mit Informationstechnologien (Weiser 1991; Weiser, Brown 1996). Für viele spezifische Anwendungen des Pervasive Computing im Gesundheitsbereich werden die beschriebenen Widersprüche nur teilweise zutreffen. Dennoch scheint eine Diskussion der Probleme, die aus zukünftigen und umfassenden Realisierungen des Pervasive Computing resultieren, gerade in Zusammenhang mit medizinischen Anwendungen

angebracht. Die Sensibilität medizinischer Daten verlangt nach einer kritischen Analyse, die in jedem einzelnen Fall zu hinterfragen hat, inwieweit die generellen Bedenken zutreffen bzw. wo Abwägungen der Vorteile mit den Eingriffen in die Privatsphäre notwendig sind.

Die Gefahren für die Privatsphäre werden von EntwicklerInnen und WissenschaftlerInnen im Bereich Pervasive Computing weitgehend gesehen und anerkannt. Beträchtliche Forschungsanstrengungen werden unternommen, um allgegenwärtige Informationstechnologien zu entwickeln, welche die Privatsphäre respektieren. Eine Gruppe von Beispielen für diese Anstrengungen umfassen Identitätsmanagementtechnologien – etwa in Form von PDAs (Personal Digital Assistants) oder Softwareagenten, welche die Privacy-Präferenzen ihrer NutzerInnen verwalten. Eine andere Gruppe umfasst die Technologien des Digital Rights Managements (DRM), etwa um eine unkontrollierte Weitergabe und Verarbeitung von generierten Daten zu verhindern.

Was aber fehlt, ist ein überzeugendes Konzept für die Gestaltung von „Pervasive-Computing-Systemen", das ein akzeptables Niveau an Privatsphäre in der Zukunft garantieren könnte. Die meisten der heute diskutierten Ansätze können die zukünftigen Technologien – in einem beschränkten Ausmaß – weniger „privacy-invasiv" ausformen. Sie sind jedoch unzureichend, um das inhärente Privatsphären zerstörende Potenzial zu überwinden. Andere Ansätze bergen wieder neue Bedrohungen für die Privatsphäre in sich, indem sie etwa auf einer verpflichtenden Identifikation aller Datensubjekte bzw. betroffenen Personen aufbauen. Aber auch im Falle von pseudonymisierten Datenzuordnungen[2] mit Hilfe von Identitätsmanagementtechnologien sind wirksame Schutzmaßnahmen kaum vorstellbar, sofern nicht alle Daten und Spuren endgültig gelöscht werden. Diese müssten nämlich einer Re-Personalisierung von pseudonymen Daten durch fortgeschrittene Verfahren der Datenanalyse und des Data-Mining oder einer nachträglichen biometrischen Identifikation widerstehen können. Ein wesentlicher Grund für die beschränkten Möglichkeiten, privacy-freundliche Pervasive-Computing-Systeme zu gestalten oder sie sich auch nur vorstellen zu können, ist in den Widersprüchen zu den wichtigsten Prinzipien des gegenwärtigen Datenschutzes begründet.

1.1 Widersprüche zu den Fundamenten von Privacy

Der Schutz der Privatsphäre ist eine zentrale Komponente der Menschenrechte. Dementsprechend ist er sowohl in der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen (Art. 12) und in der Grundrechtscharta der Europäischen Union (Art. 7 und 8) festgeschrieben. Menschenrechte genießen besonderen Schutz in den Verfassungen demokratischer Staaten, in denen sie als unveränderliche Prinzipien verankert sind oder zumindest dadurch abgesichert sind, dass besonders hohe Anforderungen an ihre Veränderung und Anpassung geknüpft sind, um sie vor politischer Willkür zu bewahren.

Die erwähnten Artikel beschreiben das Recht auf Privatsphäre in so allgemeiner Weise, dass sie keine detaillierten Untersuchungen von möglichen Inkompatibilitäten und Widersprüchen zwischen Pervasive Computing und diesem Grundrecht zulassen. Für diesen Zweck muss man auf konkrete Empfehlungen oder rechtliche Normen zurückgreifen, die in Zusammenhang mit der Anwendung von Informationstechnologien entwickelt wurden. In diesem Bereich wurden Widersprüche zwischen der technischen Entwicklung und diesem Grundrecht schon früh offenbar. Im Folgenden werden die wichtigsten Bedingungen und Vorschriften aus den OECD-Privacy-Guidelines (OECD 1980) und der EU-Datenschutzrichtlinie 95/46/EC (Europäisches Parlament und der Rat 1995) mit inhärenten Eigenschaften von Pervasive-Computing-Systemen verglichen. Obwohl rechtlich nicht verbindlich, haben die OECD-Richtlinien, die seit einem Vierteljahrhundert unverändert gültig sind, in viele freiwillige Vereinbarungen und gesetzlich abgesicherte Regulierungen Eingang gefunden, darunter auch in die erwähnte Datenschutzrichtlinie der EU. Die OECD-Richtlinien legen acht Grundsätze für den Schutz der Privatsphäre fest (OECD 2003). Dies sind die Grundsätze der

- begrenzten Datenerhebung,
- Datenqualität,
- Zweckbestimmung,

- Nutzungsbegrenzung,
- Sicherung,
- Offenheit,
- Rechenschaftspflicht und des
- Mitspracherechts.

1.2 Diskussion ausgewählter Grundsätze der OECD-Richtlinie

Konflikte zwischen den Visionen von allgegenwärtigen Informationstechnologien und den OECD-Richtlinie können für alle acht Grundsätze, die in dieser Richtlinie benannt werden, identifiziert werden (Čas 2002). Die nachfolgende Diskussion konzentriert sich aber auf die ersten vier dieser Prinzipien. Sie sind wichtiger, da sie unverzichtbare Säulen darstellen, auf denen alle gegenwärtigen Bestimmungen zum Schutz der Privatsphäre ruhen.

Grundsatz der begrenzten Datenerhebung

Bereits die Grundidee von Pervasive-Computing-Infrastrukturen widerspricht diesem Grundsatz vollständig. Daten über Personen oder Objekte innerhalb der Reichweite von Pervasive-Computing-Systemen werden aktiv, umfassend und andauernd gesammelt. Selbst wenn nur ein kleiner Teil dieser riesigen Mengen an Informationen tatsächlich gespeichert oder analysiert wird, werden die Prinzipien der Beschränktheit und Zweckbindung von Datensammlungen in ihr Gegenteil verkehrt. Der zweite Teil dieses Prinzips bezieht sich auf ein bewusstes und informiertes Einverständnis derjenigen Personen, deren Daten gesammelt werden. Während es grundsätzlich möglich scheint, dafür Bewusstsein zu schaffen (z. B. durch klar sichtbare Warnhinweise, welche anzeigen, dass Pervasive-Computing-Systeme in Verwendung sind), werden detaillierte Informationen darüber, welche Objekte welche Daten zu welcher Zeit erfassen, nicht mehr möglich sein. Diese sind sowohl aus praktischen Gründen als auch wegen der Inkompatibilität mit dem Ziel der Unaufdringlichkeit ausgeschlossen.

Eine der Anforderungen des Artikels 7 der Europäischen Datenschutzrichtlinie wird so völlig unerreichbar: die Verpflichtung, jede Bearbeitung persönlicher Daten an das ausdrückliche Einverständnis der betroffenen Person zu knüpfen. Auch heute ist die Bedingung, dass die „… betroffene Person … ohne jeden Zweifel ihre Einwilligung gegeben“ hat (Europäisches Parlament und der Rat 1995), nicht in allen Fällen und jederzeit erfüllbar und durch eine Reihe von Ausnahmen abgeschwächt. Beispiel hierfür sind Datenverarbeitungen, um vertragliche Vereinbarungen zu erfüllen, um vitale Interessen der betroffenen Person zu schützen oder bei denen ein überwiegendes öffentliches Interesse besteht.

Das Verhältnis zwischen der Möglichkeit einerseits, ein explizites Einverständnis der betroffenen Personen herzustellen, und den Überwachungskapazitäten von Pervasive Computing andererseits, verspricht in dramatischer Weise aus dem Gleichgewicht zu geraten. Jene Teile der Bevölkerung, die nicht permanent überwacht werden möchten, können natürlich ihre Unterschrift unter entsprechende Verträge verweigern und sich dadurch von der Nutzung angebotener Dienstleistungen ausschließen, jedoch besteht in einer idealen Pervasive-Computing-Welt kein Weg, der allgegenwärtigen Überwachung selbst zu entkommen. Allgegenwärtige Informationstechnologien werfen daher schwierige rechtliche Fragen auf – etwa die, ob ein „zweifelsfreies Einverständnis“ zu etwas Unvermeidbarem überhaupt ein gültiger Teil von individuellen oder kollektiven Übereinkünften sein kann.

Grundsatz der Datenqualität

Dieser Grundsatz umfasst ebenfalls zwei Dimensionen: Erstens müssen die Daten korrekt, vollständig und aktuell sein, zweitens müssen personenbezogene Daten ihrer Zweckbestimmung entsprechen. Die letztgenannte Dimension wird bei den beiden nachfolgenden Prinzipien noch näher ausgeführt. Im Allgemeinen könnte erwartet werden, dass allgegenwärtige Informationstechnologien bei der ersten hier angesprochenen Dimension zu besseren Resultaten führen werden. Es wird aber erst nach genauer Kenntnis der eingesetzten Systeme und der Auswertung empirischer Daten tatsächlicher Anwendungen möglich sein, begründete Aussagen über Aspekte der Datenqualität zu treffen. Wenn zum Beispiel die betroffenen Personen mittels biometrischer Methoden identifiziert werden, so ist ein be-

stimmter Anteil an Fehlzuordnungen von Daten zu Personen unvermeidbar. Eine Abnahme der fälschlicherweise identifizierten Personen (FAR – false acceptance rate) impliziert immer einen Anstieg der fälschlicherweise abgewiesenen Personen (FRR – false rejection rate) und umgekehrt. Darüber hinaus bedeutet ein Mehr-an-Daten nicht notwendigerweise bessere Daten. Um zu genaueren Daten zu gelangen, müssen regelmäßige Überprüfungen und Korrekturen vorgesehen werden. Dies ist aber ohne zentrale oder zumindest koordinierte Speicherung der Daten kaum vorstellbar; zentralisierte Formen der Datenspeicherung wiederum sind mit einem entsprechenden Missbrauchsrisiko behaftet.

Grundsatz der Zweckbestimmung

Im Zentrum dieses Prinzips steht die Anforderung, dass spätestens zum Zeitpunkt der Datenerhebung deren Zweck bekannt und identifizierbar sein muss. Nachfolgende Veränderungen dieses Zweckes sind nur erlaubt, wenn sie mit den ursprünglichen Intentionen vereinbar sind. Darüber hinaus müssen diese Veränderungen entsprechend bekannt gegeben werden.

Das Ziel von pervasiven Informationstechnologien ist es aber nicht, einem einzelnen Zweck zu dienen, sondern den NutzerInnen in einer Vielzahl von – mehr oder weniger vorhersehbaren – Situationen zu unterstützen. Die Abwesenheit von präzisen Definitionen über mögliche Nutzungen impliziert auch, dass zahllose Szenarien über mögliche Anwendungen von Pervasive-Computing-Systemen entwickelt werden können. Es besteht jedoch kein Wissen darüber, welche Dienste auf genügend große Nachfrage stoßen oder über akzeptable Relationen zwischen Kosten und Nutzen verfügen werden. Diese Kritik betrifft aber eine Vielzahl neuer Technologien und wäre allein noch kein ausreichender Grund für prinzipielle Bedenken gegenüber Pervasive Computing.

Das grundsätzliche Problem von Pervasive Computing ist, dass der Grundsatz der Zweckbestimmung auf den Kopf gestellt und damit ein zentrales Fundament des gegenwärtigen Datenschutzes beseitigt wird. Der Zweck der Datensammlung liegt hier ausschließlich in der Anhäufung von so vielen Informationen über individuelle Verhaltensmuster und Präferenzen wie möglich. Der Kontext und der Zweck, in dem bzw. für den dieses Wissen angewendet werden wird, bleiben zum Zeitpunkt der Datenerfassung notwendigerweise unbekannt. Diese Unmöglichkeit, einen Zweck zu nennen, macht es auch unmöglich, dies zu fordern und stellte so eine grundsätzliche Verletzung dieses Prinzips dar. Jeder Versuch, diesen Grundsatz dennoch aufrechtzuerhalten, würde aus praktischen Gründen scheitern und dem Ziel widersprechen, unaufdringliche Pervasive-Computing-Systeme zu schaffen.

Grundsatz der Nutzungsbegrenzung

In Ergänzung zum Prinzip der Zweckbestimmung besagt dieser Grundsatz, dass Daten nicht offen gelegt, bereitgestellt oder genutzt werden dürfen, wenn dies nicht den Zwecken entspricht, die zum Zeitpunkt der Datenerhebung festgelegt worden sind. Ausnahmen von diesem Grundsatz sind möglich, wenn die betroffene Person einwilligt oder wenn die Bearbeitung im Rahmen gesetzlicher Bestimmungen erfolgt.

Das Fehlen einer anfänglichen Zweckbestimmung macht es auch unmöglich, Grenzen für sekundäre Nutzungen zu ziehen. Fundamentale und unvermeidbare Widersprüche zwischen den Prinzipien der Nutzungsbegrenzung und Zweckbestimmung einerseits und den Visionen von Pervasive Computing andererseits sind darüber hinaus in der technischen Gestaltung dieses Systems begründet. Die spontane Vernetzung von zahllosen und unsichtbaren Computern sowie der Austausch von Daten zwischen ihnen sind zentrale und unverzichtbare Komponenten von derartigen Infrastrukturen. Abgesehen von technischen Problemen, die eine Begrenzung des Transfers und der Nutzung von Daten mit sich bringen würde, wäre jeder Versuch, den Grundsatz der Nutzungsbegrenzung zumindest teilweise durchzusetzen, mit entsprechenden Einschränkungen beim Nutzen und der Benutzbarkeit von Pervasive Computing verbunden.

Der Nutzen wäre beschränkt, weil vorgegebene Zuordnungen von Daten zu Anwendungen auch die Anpassungs- und Lernfähigkeit der Systeme beschränken würden. Die Benutzbarkeit wäre es, weil ständige Nachfragen zum Einverständnis oder zu Ablehnung von Datentransfers wohl innerhalb kürzester

Zeit die Grenzen der Zumutbarkeit überschreiten würden.

2 Zum Spannungsverhältnis von Datenschutz und Anwendungen

Eine Übertragung der sehr negativen Bewertung von Pervasive-Computing-Technologien aus datenschutzrechtlicher Sicht auf deren Einsatz im Gesundheitssektor wird von zwei gegensätzlich wirkenden Faktoren beeinflusst. Zum einen sind die erfassten Daten prinzipiell von sensibler Natur – zumindest insofern, als dabei Gesundheitsdaten von PatientInnen betroffen sind. Zum anderen ist aber mit diesen Anwendungen ein Zweck verbunden, der diese Eingriffe zuerst einmal gerechtfertigt erscheinen lässt. Je spezifischer der jeweilige Zweck ist, desto weniger wahrscheinlich wird es, dass Datenschutzaspekte negativ ins Gewicht fallen. Dafür sind mehrere Gründe verantwortlich: Erstens wird das Prinzip der Zweckbindung nicht verletzt, zweitens lassen sich in spezifischen Anwendungskontexten technische und organisatorische Maßnahmen zum Schutz der Daten einfacher realisieren. Insbesondere bei den zahlreichen Möglichkeiten klinischer Anwendungen von Pervasive Computing (Bardram et al. 2007) lässt sich ein effektiver Einsatz von Privacy-Enhancing-Technologies erwarten. Der Einsatz findet hier in abgegrenzten Einheiten statt, bestehende Organisationsstrukturen und Kontrollmechanismen lassen sich auf neue Technologien übertragen und, sofern PatientInnen betroffen sind, sind die Datenverarbeitungen auch zeitlich begrenzt. Viele der mit der ursprünglichen Vision von Ubiquitious Computing verbundenen Datenschutzprobleme treffen für diesen begrenzten Anwendungsbereich einfach nicht zu. Daher stellt sich die Frage, inwieweit für diese Kategorie Bezeichnungen wie „Pervasive“ oder „Ubiquitious Computing“ überhaupt gerechtfertigt sind (Korhonen, Bardram 2004) oder ob es sich dabei nicht um technische Weiterentwicklungen von Informationstechnologien handelt, welche einzelne Elemente aus dem Pervasive Computing integrieren, den damit verbundenen Paradigmenwechsel aber nicht mitvollziehen.

Grundsätzlich problematischer werden Anwendungen, wenn sie den extramuralen Bereich einbeziehen. Ein Beispiel dafür sind Systeme des Wearable Computing zur Überwachung von Vitaldaten von Patienten (Lukowicz et al. 2004). Dabei können eine Reihe von relevanten Gesundheitsdaten von Risikopatienten permanent erfasst und ausgewertet werden. Werden kritische Grenzwerte erreicht, können solche Systeme selbsttätig die notwendigen Schritte für eine medizinische Versorgung einleiten. Fortgeschrittene Systeme versuchen, durch die Einbeziehung des Kontextes, Fehlalarme zu vermeiden, indem sie etwa unterscheiden, ob eine erhöhte Pulsfrequenz auf körperliche Aktivität oder auf ein medizinisches Problem zurückzuführen ist. Umso mehr Vitaldaten und Kontextinformationen erfasst werden, desto aussagekräftigere Profile lassen sich erstellen, die über den medizinischen Bereich hinausgehen, indem sie etwa Aufenthaltsorte einbeziehen oder Rückschlüsse auf Trink- und Essgewohnheiten zulassen.

Bestrebungen, die Zeitspanne des selbstständigen Lebens mittels „Smart Homes“[3] zu verlängern, stellen eine dritte wichtige Kategorie von Anwendungen des Pervasive Computing im Gesundheitssektor dar. Wenngleich sie örtlich begrenzt sind, entsprechen diese Konzepte durch den Anspruch, alle Bereiche des täglichen Lebens im Alter oder bei Behinderung zu unterstützen, der Idee des Ubiquitous Computing am ehesten. Sie bedingen eine permanente Beobachtung der Aktivitäten, die sich nicht auf medizinische Daten beschränkt. Auf diese Weise soll auch bei Stürzen oder bei ungewöhnlich langen Phasen von Nichtaktivität ein Alarm ausgelöst werden. Dabei wird in der Regel den Alarmzentralen eine Möglichkeit geboten, von der Ferne Kontakt aufzunehmen und in die betroffenen Räume hinein zu hören oder hinein zu sehen, um durch Fehlalarme ausgelöste Einsätze zu minimieren. Diese Möglichkeit ist auch bei heutigen Senioren-Alarmsystemen vorgesehen, allerdings ist dazu eine aktive Auslösung des Alarms durch die betroffene Person notwendig. Diese Wahlfreiheit, die aber auch das Risiko beinhaltet, dass ein pflegebedürftiger Mensch nicht mehr in der Lage sein kann, den Alarm auszulösen, ist in diesem Fall nicht mehr gegeben.

Optionen zum Datenschutz

Die breite Palette von möglichen Anwendungen von Pervasive Computing im Gesundheitswesen verlangt nach spezifischen technischen und organisatorischen Maßnahmen im konkreten Einzelfall. Ganz generell ist dabei nach den geltenden Prinzipien des Datenschutzes zu verfahren. Ein zentrales Anliegen bleibt die Minimierung der erhobenen und verarbeiteten Daten. Angesichts der ständig steigenden Leistungsfähigkeit von Sensoren, Speicher- und Prozessorkapazitäten besteht hier die Versuchung, mehr Daten mit mehr Qualität bei der medizinischen oder pflegerischen Betreuung gleichzusetzen. Hier sind Vorkehrungen gefordert, die Bedürfnisse der Betroffenen – sowohl der PatientInnen als auch des medizinischen und pflegerischen Personals – aktiv in die Forschungs- und Entwicklungsphase von Systemen des Pervasive Computing einzubeziehen.

Ein weiterer zentraler Punkt ist die Sicherung der sensiblen Daten vor unberechtigtem Zugriff. Zu diesem Zweck sind ausgereifte technische Systeme der Zugriffskontrolle und Protokollierung notwendig und auch verfügbar, diese können aber dem Leitbild der Unaufdringlichkeit widersprechen. Spezifische Probleme könnten auch mit dem Ziel der universellen und schnellen Verfügbarkeit von medizinischen Daten verbunden sein, wenn etwa MitpatientInnen oder zufällig anwesende Personen Einblick in Informationen erhalten, die über großflächige im Klinikbereich verfügbare Displays angezeigt werden. Restriktive Vorgaben sind auch für die Weitergabe von Daten an externe Organisationen (wie Kostenträger, Versicherungsunternehmen oder private Dienstleister) im Bereich häuslicher Pflege- und Assistenzleistungen vorzusehen, um den Prinzipien der Zweckbestimmung und Nutzungsbegrenzung gerecht zu werden. Genaue Abwägungen sind notwendig

Technologien des Pervasive Computing treten mit dem doppelten Heilsversprechen an, sowohl die Qualität medizinischer Dienstleistungen zu erhöhen als auch deren Kosten zu senken. Eine gründliche Evaluierung und Überprüfung dieser Annahmen in Pilotversuchen ist für eine Einführung dieser Technologien in den Gesundheitssektor unumgänglich, die das Grundrecht auf Privatsphäre respektiert und achtet. Angekündigte Verbesserungen von medizinischen und pflegerischen Leistungen, noch dazu zu geringeren Kosten, können leicht dazu verleiten, die Akzeptanz für Eingriffe in die Privatsphäre über ein angebrachtes Maß hinaus zu erhöhen.

Die Notwendigkeit einer kritischen Analyse soll anhand einiger Beispiele illustriert werden.

Eine breite Einführung von Pervasive-Computing-Technologien in den Gesundheitsbereich bedeutet eine weitere Technisierung der Medizin. Zweifelsohne werden sich hinreichend Beispiele finden lassen, bei denen genauere und schneller verfügbare medizinische Daten eine Verbesserung der Behandlungsqualität erlauben würden. Dennoch ist eine Verallgemeinerung dieser Beispiele unzulässig. Mehr und bessere Daten könnten dazu verführen, diesen mehr Vertrauen und Aufmerksamkeit zu schenken, als dem subjektiven Empfinden der PatientInnen. Selbst wenn dies aus medizintechnischer Sicht gerechtfertigt erscheint, kann es dennoch das Arzt-Patient-Verhältnis nachhaltig trüben und im Sinne ganzheitlicher Ansätze der Medizin den Behandlungserfolg mindern oder verhindern.

Sowohl von einer besseren Nutzung von personellen Ressourcen als auch von medizinischen Apparaten werden qualitative Verbesserungen und Kosteneinsparungen erwartet. Während sich bei Apparaten dieses Verhältnis durchaus rational begründen lässt, ist eine Übertragung auf ärztliches oder pflegerisches Personal zu hinterfragen. Natürlich werden sich im Einzelfall Möglichkeiten finden lassen, unproduktive Phasen zu verringern. Eine Gleichsetzung von Menschen mit Maschinen, die keine Ruhepausen benötigen, um Produktivität und Qualität aufrechterhalten zu können, ist aber unzulässig. In manchen Fällen ist es gerade umgekehrt. Es sind die unproduktiven Phasen wie die Bereitschaftsdienste, die einen wesentlichen Beitrag zur medizinischen Basisversorgung und Sicherheit der Bevölkerung leisten. Vielfach scheinen auch die Erwartungen an den Einsatz von Pervasive Computing überzogen zu sein. So ist zumindest zu hinterfragen, ob der zusätzliche technische Aufwand der permanenten Lokalisierung medizinischen Personals den im Vergleich zu herkömmlichen Pager-Diensten erzielbaren Vorteil rechtfertigt.

Fortschritte in der Medizin und der Medizintechnik sind ein unverzichtbarer Bestandteil besserer medizinischer Behandlungsmöglichkeiten mit gravierenden Verbesserungen der Lebensqualität und Lebenserwartung – zumindest bei jenen Personen, die von diesen Fortschritten profitieren können. Kosteneinsparungen zählen allerdings nicht zu den Effekten, die üblicherweise mit den neuen Möglichkeiten der Medizin in Verbindung gebracht werden. Es ist auch nicht unmittelbar einsichtig, warum dies bei Pervasive-Computing-Anwendungen anders sein soll. So ist es durchaus vorstellbar, dass eine Ausweitung der permanenten Überwachung von Vitaldaten auch die Grenzen zwischen „gesund" und „krank" verschiebt. Dies könnte zumindest einen Teil der Einsparungen, die aus verkürzten stationären Aufenthalten resultieren, wieder zunichte machen. Dies wird wahrscheinlich oft der Fall sein, da die Grenzwerte für eine Alarmauslösung niedrig angesetzt werden müssen, um ein Vertrauen in diese Systeme zu rechtfertigen und mögliche Schadenersatzklagen zu vermeiden.

3 Fazit

Eine einfache Gleichsetzung von mehr Technik mit mehr Qualität ist wenig hilfreich, um eine Abwägung der damit verbundenen Eingriffe in die Privatsphäre zu erlauben. Zuvor müsste jeweils zumindest geklärt werden, wie Qualität im medizinischen und pflegerischen Bereich zu verstehen ist: Dominiert die technische oder die menschliche Komponente und inwieweit gelingt es, ein ausgewogenes Verhältnis zu erreichen? Es ist auch ganz generell zu hinterfragen, ob Kostenargumente allein genommen als Steuerungsinstrumente im Medizinsektor hinreichend sein können. Damit soll nicht gesagt werden, dass Kostenaspekte nicht wichtig wären. Im Gegenteil: Selbstverständlich müssen öffentliche Mittel effizient verwendet werden. Wie viele Mittel aber für das Gesundheitswesen zur Verfügung gestellt werden, und auf welche Weise diese finanziellen Ressourcen rekrutiert werden, ist eine gesellschaftspolitische Entscheidung, die einer breiten und informierten Debatte bedarf.

Anmerkungen

1) Dieser Abschnitt beruht auf einer stark gekürzten deutschen Fassung meines Beitrags „Privacy in Pervasive Computing Environments – A Contradiction in Terms?" (Čas 2004). Eine ungekürzte Fassung wurde in „Technikfolgenabschätzung in der österreichischen Praxis. Festschrift für Gunther Tichy" (Nentwich, Peissl 2005) veröffentlicht.
2) Eine anonymisierte Erfassung von Daten ist nicht geeignet, um Dienste anbieten zu können, die an die Bedürfnisse der jeweiligen Person angepasst sind. „Pseudonymisiert" bedeutet in diesem Sinn, dass diese Daten an ein Pseudonym und nicht an die wahre Identität einer Person geknüpft sind.
3) Hier ist eine spezielle Form von Wohnungen gemeint, welche mit intelligenter Haustechnik zur Unterstützung älterer Personen ausgestattet sind; Beispiele sind etwa Herdplatten, die sich automatisch abschalten oder Sensoren, die Stürze erfassen oder bei längerer Bewegungslosigkeit selbsttätig Hilfe herbeirufen.

Literatur

Bardram, J.E.; Baldus, H.; Favela, J., 2007: Pervasive Computing in hospitals. In: Bardram, J.E.; Mihailidis, A.; Wan, D.; Raton, B. (Hg.): Pervasive Computing in Healthcare. Boca Raton, FL, S. 49-77

Č*as, J.*, 2002: UC – Ubiquitous Computing oder Ubiquitous Control? In: Britzelmaier, B.; Geberl, S.; Weinmann, S. (Hg.): Der Mensch im Netz – Ubiquitous Computing. Stuttgart, S. 39-52

Č*as, J.*, 2004: Privacy in Pervasive Computing Environments – A Contradiction in Terms? IEEE Technology and Society Magazine 24/1 (2004), S. 24-33

Europäisches Parlament und der Rat, 1995: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Amtsblatt Nr. L 281 vom 23.11.1995, S. 0031-0050; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html (download 5.5.08)

Korhonen, I.; Bardram, J.E., 2004: Guest Editorial Introduction to the Special Section on Pervasive Healthcare. IEEE Transactions on Information Technology in Biomedicine 8/3 (2004), S. 229-234

Lukowicz, P.; Kirstein, T.; Troster, G., 2004: Wearable systems for health care applications. In: Methods of Information in Medicine 43/3 (2004), S. 232-238

Mattern, F.; Langheinrich, M., 2001: Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller, G.; Reichen-

bach, M. (Hg.): Sicherheitskonzepte für das Internet. Berlin, S. 7-26; http://www.inf.ethz.ch/vs/publ/papers/allgegenwaertig.pdf (download 5.5.08)

Nentwich, M.; Peissl, W. (Hg.), 2005: Technikfolgenabschätzung in der österreichischen Praxis. Festschrift für Gunther Tichy, Wien

OECD – Organisation for Economic Co-operation and Development, 1980: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (download 5.5.08)

OECD – Organisation for Economic Co-operation and Development, 2003: Kurzfassung OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten; http://www.oecd.org/dataoecd/16/7/15589558.pdf (download 5.5.08)

Varshney, U., 2003: Pervasive healthcare. In: IEEE Computer 36/12 (2003), S. 138-140

Weiser, M., 1991: The computer for the 21st century. In: Sci Amer 265/3 (1991), S. 66-75; http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html (download 5.5.08)

Weiser, M.; Brown, J.S., 1996: The Coming Age of Calm Technology; http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm (download 5.5.08)

Kontakt

Johann Čas
Institut für Technikfolgen-Abschätzung
Österreichische Akademie der Wissenschaften
Strohgasse 45/3. Stock, 1030 Wien, Österreich
E-Mail: jcas@oeaw.ac.at
Internet: http://www.oeaw.ac.at/ita/

« »

Ethische Fragen des Pervasive Computing im Gesundheitswesen

von Ludwig Siep, Universität Münster

Geräte und Systeme des Pervasive Computing versprechen im Gesundheitswesen eine Reihe von Vorteilen für die Benutzer und die Gesellschaft. Für Krankenhäuser und andere medizinische Einrichtungen (z. B. die Unfallmedizin) stellen sie Verbesserungen in der Kommunikation und der Effizienz, aber auch Einsparmöglichkeiten in Aussicht. Für Kranke oder in ihren körperlichen und mentalen Funktionen Eingeschränkte bieten sie Überwachungs- und Kompensationsmöglichkeiten, die das alltägliche Leben erleichtern und ihre Selbstständigkeit bzw. Unabhängigkeit von Pflegepersonal und -einrichtungen steigern können. Neben diesen positiven Effekten sind aber auch gravierende Risiken für Sicherheit und Autonomie der Patienten sowie für die Gerechtigkeit im Gesundheitswesen erkennbar. Die ethische Reflexion sollte frühzeitig auf diese Probleme aufmerksam machen, ohne von den Entwicklungsmöglichkeiten abraten zu müssen.

Unter Pervasive Computing im Gesundheitswesen versteht man den umfassenden Einsatz von mobilen, drahtlosen, oft miniaturisierten Geräten der Datenerfassung, -verarbeitung und -übertragung im Bereich der Prävention, Diagnostik, Therapie und Krankenpflege. Auch Anwendungen im Bereich der Altenpflege oder die Verwendung technischer Geräte zum Ausgleich eingeschränkter Fähigkeiten (Hör-, Seh- oder Gehhilfen, Kompensation kognitiver Defizienzen etc.) gehören dazu. „Pervasive" bedeutet auch, dass die Geräte möglichst unauffällig und „benutzerfreundlich" in der Umgebung des Trägers – vom Körper über die Kleidung bis in die Wohnung – integriert sind („They are everywhere", Korhonen, Bardram 2004, S. 229). Zu ihrem spezifischen Charakter gehört in der Regel ihre „Intelligenz", d. h. ihre Selbstlokalisation und die Erfassung ihrer Umgebung („context awareness") sowie ihre (kybernetische) Fähigkeit, auf die erfassten Daten (vor allem dramatische Änderungen) durch