

Einführung: Wearable Computing als Problem des Datenschutzes

Kaum ein Rechtsgebiet wird so von den immer neuen Entwicklungen der Informations- und Kommunikationstechniken (I&K-Techniken) herausgefordert wie das Datenschutzrecht. Während viele neue Anwendungen mit geeigneten Konkretisierungen bestehen der Datenschutzregelungen und mit problembewussten Anpassungen der Datenschutzpraxis beherrscht werden können, wird dies für Ubiquitous Computing bezweifelt. Dringen die I&K-Techniken in alle Lebensbereiche ein und bieten sie für (fast) alle Situationen unbemerkt und ungefragt Unterstützung oder Informationen und müssen sie daher über ihre Nutzer (fast) alles wissen, sind nicht nur neue Interpretationen und Praktiken gefragt. Vielmehr wird vermutet, dass diese allgegenwärtige Datenverarbeitung das gesamte bisherige Schutzkonzept des Datenschutzrechts in Frage stellt und eine neue Konzeption der Risikoabwehr und -vorsorge erfordert.¹

Ein wichtiges Anwendungsfeld der Idee des Ubiquitous Computing ist das Wearable Computing.² In den nächsten Jahren wird Ubiquitous Computing nicht nur – wie bereits zu beobachten ist – in der näheren Umgebung des Menschen, wie etwa in der Haustechnik oder im Automobil, genutzt werden, sondern auch in der Hülle um seinen Körper oder sogar in diesem selbst eingebaut sein. Immer mehr elektronische Geräte werden in miniaturisierter Form in der Kleidung oder etwa in Armbanduhren, Brillen und Schmuckstücken enthalten sein. Sie werden vor allem genutzt werden, um die Sicherheit des Nutzers zu erhöhen, seine Sinne zu erweitern, sein Gedächtnis zu unterstützen und ihm seine Arbeit zu erleichtern.³

Wearable Computing kann die Sicherheit des Nutzers zum Beispiel dadurch erhöhen, dass seine Körper- und Umgebungsdaten zur medizinischen Kontrolle erfasst und verarbeitet werden. Für die ambulante Beobachtung von Patienten sind bereits Kleidungsstücke wie Hemden oder Anzüge entwickelt worden, in die sowohl verschiedene Sensoren als auch Speicher- und Kommunikationseinheiten integriert sind, die Vitalparameter wie Blutdruck, Herzfrequenz oder Sauerstoffverbrauch erfassen und für eine spätere

¹ S. hierzu ausführlich mit vielen Nachweisen *Roßnagel* 2007; *ders.* 2008, 123 ff.

² S. hierzu z.B. *Roßnagel* 2007, 40 ff. m.w.M.

³ S. zu diesen Träumen, die für die Nutzung von Ubiquitous Computing bedeutsam sein werden, s. *Roßnagel* 2007, 13 ff.

Untersuchung speichern oder unmittelbar an eine Kontrollstation übermitteln. Durch diese Kleidungsstücke können auch Alarme ausgelöst werden, wenn die gemessenen Werte dazu Anlass geben.

Die Sicherheit des Anwenders wird auch erhöht, wenn durch Chips in der Kleidung der Aufenthaltsort jedes Mitarbeiters oder jedes in einem bestimmten gefährlichen Bereich befindlichen Menschen festgestellt werden kann.⁴ Sensoren können riskante Situationen erkennen und den Nutzer vor diesen warnen. Ein anderes Beispiel könnte eine Alarmfunktion sein, die Gegenstände in Jacke oder Hose vor Diebstahl schützen.

Wearable Computing wird die Sinne des Nutzers verstärken, indem Sensoren ihn unterstützen, die Umgebung wahrzunehmen. Künftig dürfte es Brillen geben, in die beinahe unbemerkt ein Mikrofon, eine Kamera, Stereoton und ein GPS-System integriert sind. Diese Brille der Zukunft kombiniert Mobiltelefon und Videokamera und ist ständig mit dem Internet verbunden. Die kleine Kamera erweitert den Sehsinn des Nutzers, indem dieser durch sie im Infrarotmodus auch in der Nacht sehen, durch die Zoomfunktion wie mit einem Feldstecher auch ferne Dinge erkennen oder im Makromodus wie durch eine Lupe kleine Strukturen wahrnehmen kann.

Eng mit diesen Anwendungen zusammen hängt die Möglichkeit für den Nutzer, mit Wearable Computing sein Gedächtnis zu erweitern, indem er die Kamera und das Mikrofon in der Brille dazu verwendet, alles, was sich vor ihm akustisch oder visuell abspielt, aufzuzeichnen. Diese Aufzeichnungen können durch Orts- und Zeitstempel markiert und so leicht wieder gefunden werden. Die Daten können auf den individuellen Server des Nutzers übertragen und dort als „Tagebuch der Sinne“⁵ gespeichert werden. Mit geeigneter Software kann so prinzipiell jeder Moment im Leben in Erinnerung gerufen werden. Will der Nutzer sich an etwas erinnern, kann ihm die früher aufgenommene Situation über Kopfhörer oder über eine Projektion auf die Netzhaut vorgespielt werden. Über Gesichtserkennung könnte ihm so etwa immer die letzte Begegnung mit einem Menschen, den er gerade trifft, in Erinnerung gerufen werden.

Wearable Computing vermag schließlich viele Berufstätige bei der Erfüllung ihrer Aufgaben zu unterstützen. Vielfach benötigen sie – wie etwa Reporter, Wartungsmonteure oder Lagerarbeiter – einerseits beide Hände für ihre Tätigkeit und andererseits zugleich situations- und kontextabhängig vielfältige Informationen. Für sie wäre es sehr hilf-

⁴ S. im Folgenden das Beispiel der Schutzzanzüge für Feuerwehreinsatzkräfte.

⁵ *Maurer*, Informatik-Spektrum 2004, 47.

reich, wenn die sie umgebenden Datenverarbeitungssysteme erkennen könnten, welche Information sie benötigen, und diese ihnen über spezifische Ausgabegeräte, wie zum Beispiel die Projektion von Schaltplänen direkt auf das zu reparierende Systemteil, ausgeben.

Mit Wearable Computing kann der Benutzer durch solche Anwendungen eine auf seine persönliche Interessenlage zugeschnittene „Informations- und Funktionsaura“ mit sich herumtragen, die ihn zugleich mit der Welt verbindet.

Zur datenschutzrechtlichen Beherrschung der Risiken für die informationelle Selbstbestimmung wurde vorgeschlagen, den Einsatz von Ubiquitous oder Wearable Computing danach zu unterscheiden, ob er in überschaubaren Anwendungen stattfindet, die durch bekannte und bewertete Interessenkonflikte bestimmt sind, oder ob der Einsatz in komplexen, unübersichtlichen Situationen erfolgt, die neue Interessenkonflikte hervorrufen.⁶

Das Datenschutzrecht enthält zwar keine speziellen Regelungen für Anwendungen allgegenwärtiger Datenverarbeitung. Sein normatives Schutzkonzept dürfte jedoch für grundsätzlich tauglich befunden werden,⁷ wenn die zu bewertenden Anwendungen dadurch gekennzeichnet sind, dass

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

⁶ S. Roßnagel 2007. 120 ff.

⁷ Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 57 ff.

keiten durchschaubar sind, können der Betroffene oder die Datenschutzaufsicht sich auf das Ereignis konzentrieren und ihre Kontrollrechte geltend machen.

In solchen Konstellationen wird allgegenwärtige Datenverarbeitung Möglichkeiten der Interessendurchsetzung zwischen den Beteiligten verschieben und für die Datenverarbeiter auch neue Missbrauchsmöglichkeiten eröffnen. Dennoch entsprechen die neuen Problemstellungen dem „Erwartungshorizont“ des Datenschutzrechts und es ist weiterhin möglich, die rechtliche Erlaubnis einer Datenverwendung zu überprüfen und datenschutzrechtliche Grundsätze wie Transparenz für den Betroffenen sowie Zweckbindung und Erforderlichkeit der Datenverarbeitung zur Anwendung zu bringen. Dies wurde für die allgegenwärtige Datenverarbeitung etwa im Arbeitsverhältnis, im Versicherungsverhältnis und im Mietverhältnis näher erläutert.⁸

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

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

Auf diese neuen Verhältnisse – so wird befürchtet – sind die Grundsätze des datenschutzrechtlichen Schutzprogramms kaum anwendbar. Die Ziele, zu deren Erreichung allgegenwärtige Datenverarbeitung eingesetzt wird, widersprechen den Zielen, die mit den Prinzipien des Datenschutzrechts verfolgt werden. Im Konflikt zwischen beiden dürfte entscheidend sein, dass die Anwendungen des Ubiquitous Computing den Betroffenen in den meisten Fällen nicht aufgedrängt – in diesem Fall dürften die Datenschutzprinzipien greifen –, sondern von diesen gewollt werden. Sie wollen sich mit ih-

⁸ S. Roßnagel 2007, 123 ff.

rer Hilfe die Träume erfüllen, die Ubiquitous Computing zu erfüllen verspricht. Sie werden dann als Konsequenz auch damit einverstanden sein müssen, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweise, Gewohnheiten, Einstellungen und Präferenzen erhalten. In diesen neuen Verhältnissen wird das bisherige Schutzprogramm als solches – in jedem seiner Bestandteile – in Frage gestellt.⁹

Der Auftrag der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, ein Rechtsgutachten zur „Zulässigkeit von Feuerwehr-Schutzanzügen mit Sensoren und Anforderungen an den Umgang mit personenbezogene Daten“ zu erstellen, ermöglichte, an einem konkreten Beispiel, diese Thesen zumindest teilweise zu überprüfen.

Um die Feuerwehreinsatzkräfte in gefährlichen und unübersichtlichen Situationen besser koordinieren und schützen zu können, soll Wearable Computing in ihre Schutzanzüge integriert werden. Dadurch können Sensoren während des Einsatzes Vital- und Umgebungsparameter erheben und an die Einsatzleitung übermitteln. Diese kann mit ihrer Hilfe besser einschätzen, welchen Belastungen eine Einsatzkraft ausgesetzt ist und welchen Einsatzanforderungen sie aktuell gewachsen ist. Durch diese Form des Schutzes und der Koordination werden im Beschäftigungsverhältnis dem Arbeitgeber Informationen bekannt, die er bisher nicht kannte. Sie ermöglichen ihm nicht nur, den Einsatz besser zu steuern und die Beschäftigten besser zu schützen, sondern sie auch hinsichtlich ihrer Einsatzleistung und ihrer allgemeinen körperlichen Leistungsfähigkeit einzuschätzen.

An diesem Beispiel kann die These, dass das bestehende Datenschutzrecht bei risiko-adäquater Konkretisierung auch beim Einsatz von Ubiquitous Computing ausreichend leistungsfähig ist, wenn es sich um übersichtliche Situationen mit bekannten Interessenkonstellationen handelt, überprüft werden.

Diese Überprüfung ist zugleich ein Beitrag für den Forschungsschwerpunkt „Gestaltung technisch-sozialer Vernetzung in situativen ubiquitären Systemen“ (VENUS) des Forschungszentrums für Informationstechnik-Gestaltung (ITeG), der durch die Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE) des Landes Hessen gefördert wird. In diesem Schwerpunkt steht unter anderem die rechtliche Gestaltungsfähigkeit von Ubiquitous Computing-Anwendungen im Mittelpunkt der Forschungen. Für diese Fragestellung liefert das folgende Rechtsgutachten vielfältige Hinweise und Erkenntnisse.

⁹ S. Roßnagel 2007, 128 ff.; Roßnagel 2008, 141 ff.

Die Autoren danken der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin für die Möglichkeit, diesen praxisnahen Anwendungsfall zu untersuchen und die Ergebnisse in diesem Buch der rechtswissenschaftlichen Diskussion zur Kenntnis zu bringen.

Datenschutz bei Wearable Computing

Eine juristische Analyse am Beispiel von Schutzanzügen

Rossnagel, A.; Jandt, S.; Skistims, H.; Zirfas, J.

2012, VII, 180 S. 2 Abb., Softcover

ISBN: 978-3-8348-2554-4