Context-Awareness und rationale Risikowahrnehmung

Oliver Siemoneit

SFB 627 „Umgebungsmodelle für mobile kontextbezogene Systeme“
Institut für Philosophie
Universität Stuttgart
Seidenstraße 36
70174 Stuttgart
oliver.siemoneit@philo.uni-stuttgart.de

Abstract: Aktuelle Innovationen der Informations- und Kommunikationstechnologie (IuK), wie sie etwa unter den Schlagworten ortsbasierte Dienste bzw. intelligente Handlungsumgebungen thematisiert werden, eröffnen ein weites Spektrum neuartiger Anwendungen, deren Chancen und Risiken es dezidiert zu erörtern gilt. Anhand der Leitdifferenz subjektives vs. objektives Risiko soll eine differenzierte Analyse des herrschenden Technikdiskurses erfolgen und der Weg für eine rationale Technikbewertung als auch Technikgestaltung frei gemacht werden.

1 Problemexposition

Zweifelsohne haben die technischen Entwicklungen in den letzten Jahren eine neue Qualität der Überwachung möglich werden lassen, vor der man vor Jahren nur träumen oder aber erschaudern konnte – wie einst Georg Orwell in seinem Roman „1984“. Heutige technische Systeme, wie sie etwa im Rahmen des sog. context-aware Mobile als auch Ubiquitous Computing diskutiert werden, eröffnen die Möglichkeit einer umfangreichen, lückenlosen und detaillierten Erfassung einer Vielzahl von Kontextinformationen bzw. Daten unserer Lebenswelt, deren langfristige Speicherung, Abruf, Zusammenführung und Auswertung. Das Dilemma dieser modernen IuK-Anwendungen tritt dabei deutlich zu Tage: Auf der einen Seite sind diese Systeme auf eine umfassende Datenerfassung ihrer Kontexte angewiesen, um überhaupt die erforderlichen neuartigen Systemleistungen erbringen zu können. Auf der anderen Seite erschaffen die Systeme neben den intendierten Entlastungseffekten gleichzeitig aber auch Potentiale des Missbrauchs der erfassten Datenbestände. Technischer Fortschritt schafft damit nicht nur neue, erweiterte Handlungsoptionen bzw. Möglichkeiten, sich gegen vorhandene Gefahren und Risiken mittels dieser neuen Techniken abzusichern, sondern erzeugt seinerseits selbst neue Gefahren und Risikopotentiale, die es dezidiert zu erörtern gilt.

Die herrschende Akzeptanzlage in der Bevölkerung bezüglich des Einsatzes mobiler bzw. ubiquitärer kontextsensitiver IuK-Systeme stellt sich als äußerst fragmentiert dar und ist von Irrationalitäten durchsetzt: Auf der einen Seite werden potentielle Überwachungsstrukturen, wie sie heute etwa schon mit der Mobiltelefonie und der damit unwei-

gerlich verbundenen rudimentären Verarbeitung von Ortsdaten gegeben ist, kaum als solche wahrgenommen. Die Bereitschaft die Techniken zu nutzen scheint groß. Einschlägige Nutzungsszenarien (z.B. [Is01], [Do99]) verweisen vorwiegend auf die Darstellung der neuen Möglichkeiten und Interaktionsformen, die die Techniken für unterschiedliche soziale Akteure bieten. Auf der anderen Seite zeigen die Diskussionen aber auch, dass man zwar geneigt ist, Mobiltelefonie und Location-Based-Services zu nutzen, kaum aber die Bereitschaft besteht, die dafür notwendige Infrastruktur wegen der geglaubten Schädlichkeit von NIS-Strahlung in der Nähe des eigenen Wohnortes zu akzeptieren. Konträr zum faktischen Verhalten im Internet wird Privatheit und dem Schutz personenbezogener Daten bei gezieltem Nachfragen oft eine hohe Bedeutung beigemessen und als wesentliche zu erfüllende Anforderung an technische Systeme formuliert.

Damit einher geht der Trend, dass der Begriff der Überwachung nicht mehr vorwiegend negativ konnotiert wird, sondern als integraler Bestandteil und Selbstverständlichkeit einer modernen Gesellschaft betrachtet wird. Nicht nur werden staatlichen Organisationen heute weitgehende Überwachungsmöglichkeiten eingeräumt (einseitig-asymmetrische Form der Überwachung), sondern die Bereitschaft der Bürger, sich aufgrund des Rückzuges des Staates untereinander selbst zu überwachen, steigt zusehends (Privatisierung, Zunahme der gegenseitigen, symmetrischen Überwachung). Überwachbarkeit bzw. Überwachung und die damit verbundenen Einschränkungen der Privatsphäre werden zur Abwehr bestimmter geglaubter Gefahrenlagen hier billigend in Kauf genommen.

2 Subjektive Gefahrenwahrnehmung und objektives Risiko

Unsere moderne technische Kultur hat die Gefahren des Lebens drastisch verringert. Gefahrenminimierung ist neben Nutzenmaximierung damit wohl das wichtigste Motiv, um technische Innovationen anzuregen und durchzusetzen. Analysiert man die Technikgenese des Ubiquitous Computing und dessen Determinaten, wird deutlich, dass dem Argument der Gefahrenabwehr eine hohe Bedeutung zukommt. Dem Einsatz neuer Techniken zum Aufbau von Datenbeständen als auch der Umwidmung bereits vorhandener Datenbestände – etwa die geplante polizeiliche Auswertung von Mautdaten (bzw. der für Abrechungszwecke gespeicherten Verbindungsdaten) – wird häufig unter dem Argument der Wahrung der Sicherheit zugestimmt. Dabei ist man jedoch unweigerlich mit folgendem Paradox konfrontiert: Erst moderne Technik erlaubt uns die hohen Standards an Sicherheit, an die frühere Generationen kaum zu denken wagten. Die Tatsache aber, dass diese Standards in vielen Fällen relativ gut erfüllbar sind, weckt zugleich neue Erwartungen bezüglich höherer Sicherheitsstandards, die den Bedarf an neuen Maßnahmen aufzeigen, zugleich aber auch vor Augen führen, dass es vollständige Sicherheit nicht geben kann. Will man nicht anerkennen, dass Unwägbarkeiten, Gefahren, Risikopotentiale einen Grundzug der menschlichen Existenz darstellen, die es von freien Menschen in einem gewissen Maße zu tragen und ertragen gilt, führt dies häufig in eine Spirale von Sicherheitsmaßnahmen und Ausnahmeregelungen, um endlich die erwünschte Sicherheit herzustellen, die letztendlich jedoch eine Illusion bleiben muss („slippery slope“-Situation). Ein Ausweg aus dieser Situation im Rahmen einer Technikbewertung und eines rationalen Diskurses ist es, statt auf subjektives Empfinden auf die objektiv gegebene Gefahrenlage abzuheben. D.h.: Moderne, technisch verfasste Gesellschaften

sollen sich von der subjektiven Gefahrenwahrnehmung zur rationalen Risikobeurteilung weiterbilden, indem das Produkt aus kalkulierter Eintrittswahrscheinlichkeiten und Schadenshöhen verschiedener Gefahrenpotentiale objektiv miteinander verglichen werden. Risikovergleiche dienen dann der Klärung der sog. *Akzeptabilität* von Handlungen und technischen Innovationen. *Akzeptanz* hingegen beschreibt die faktische, empirisch-sozialwissenschaftlich beschreibbare Bereitschaft eines Individuums oder einer Gruppe, gewisse Handlungen zu vollziehen bzw. gewisse technische Systeme zu nutzen. Faktische Akzeptanzlagen sind oft irrational, gezeichnet von Unwissen, Widersprüchen, Inkonsistenzen und können somit kaum eine tragfähige Entscheidungsbasis abgeben. So werden etwa gewohnte Risiken (Verkehrsteilnahme), schleichende Risiken (Rauchen), gut wahrnehmbare Risiken und aktiv selbst eingegangene Risiken oft stark unterbewertet (vgl. [Hu95], S. 97). Überbewertet werden dagegen oft unsichtbare Risiken (Elektrosmog), passive Betroffenheitsrisiken (Asbest) und Großschadensereignisse (Flugzeugabsturz, Terroranschlag) (vgl. [Hu95], S. 97). Für das vorliegende Thema bedeutet dies: Das Risiko Opfer eines Gewaltverbrechens bzw. einer terroristischen Aktivität zu werden, wird generell eher überschätzt. Gleichzeitig wird – wie die TAUCIS Studie in einer empirischen Umfrage belegt hat, das Risiko des Datenmissbrauchs und das Opfer von Überwachungsmaßnahmen zu werden – sei es von staatliche oder auch wirtschaftlicher Seite – deutlich unterschätzt (vgl. [Bi06], S. 176ff.). Schleichende Risiken, wie etwa das Hineinwachsen in eine potentielle Überwachungsstruktur bzw. selbst eingegangenen Risiken etwa in Form der Entscheidung über die Freigabe persönlicher Daten im Zuge der Nutzung lokationsbasierter Dienste oder das Einstellen persönlicher Informationen in das Internet, scheinen in ihrer Tragweite durchweg eher unterschätzt zu werden.

Der objektive Risikovergleiche, anhand dessen die begründete, konsistente Akzeptabilität erörtert werden kann, scheint in Gesellschaften, die sich rational organisieren wollen, daher unverzichtbar. Die bereits angedeutete Argumentationslinie stellt sich in Gänze damit wie folgt dar:

(1) Anhand der Leitdifferenz subjektives vs. objektives Risiko sollte im Zuge der Einführung ubiquitärer IuK-Techniken eine differenziertere Analyse von Gefahrenlagen erfolgen, denn subjektiv gefühlte Bedrohungen entsprechen nicht unbedingt den objektiv-rechnerischen Gefahrenlagen, tatsächlich Opfer eines bestimmten Gefahrenpotentials zu werden.

(2) Unsicherheit und Unwägbarkeiten ausgeliefert zu sein, ist Grundzug der menschlichen Existenz. Freiheit bedeutet, sich diesen Gefahren und Risiken bewusst zu sein, diese anzuerkennen und sich der Gefahr des Getroffen-Werdens auszusetzen. Sonst ist der Mensch unfrei, Opfer und Getriebener irrationaler Gefühle der Kleinheit, Angst und Ohnmacht gegenüber der Welt. Unfreiheit beginnt nicht erst da, wo Gesetze persönliche Freiheitsrechte und das Recht auf informationelle Selbstbestimmung einschränken, sondern in der inneren irrationalen Abhängigkeit geglaubter Gefahrenlagen, die einem rationalen Umgang mit der Problematik im Weg stehen.

(3) Unterbleibt dieser Anerkennungsakt, dass Gefahren und Risiken grundlegende Bestandteile unseres Lebens sind, findet das Streben nach Sicherheit erneut Nahrung in anderen Lebensbereichen, führt dem Betroffenen aber zugleich vor Augen, dass die von ihm angestrebte allumfassende Sicherheit nicht zu haben ist. Diese Einsicht bewirkt oft eine noch stärkere Verunsicherung des Betroffenen, die ihn dazu verleitet, weitere Sicherungsmaßnahmen einzufordern.

(4) Mit Einführung gewisser Sicherungsmaßnahmen dank neuartiger IuK-Techniken ist ferner zu fragen, ob neben der offensichtlichen Reduktion bestimmter subjektiver als auch objektiver Gefahrenlagen nicht auch neue Gefahren und Risikopotentiale geschaffen werden, die den Befürwortern des Einsatzes der neuen Technik zunächst nicht in den Blick geraten, sich bei näherer Hinsicht als weit gefährlicher und risikoträchtiger für das Gesamtsystem erweisen, als die ursprünglichen (Umwidmung und Zusammenführung heterogener Datenbestände, gläserner Bürger).
(5) Schließlich kann das Plädoyer für einen rationalen Risikovergleich auf Basis objektiv festgestellter Risiken als Killerargument gegen ein ökonomisches Nutzenkalkül erweisen, persönliche Privatheit im Zuge des Erhalts von Gegenleistungen und Services einzuschränken. Dies liegt daran, dass die Nutzenkalkulationen vorwiegend auf subjektiver Basis und geglaubter Nutzenwerte ansetzten, selten jedoch einen objektiven Risikovergleich als Entscheidungsbasis mit einbezieht, womit die Entscheidung aus Perspektive des objektiven Risikovergleichs als nicht vollständig rational zu charakterisieren ist. In den aktuellen Diskussionen findet diese Erkenntnis Niederschlag in der Forderung, dass mehr Aufklärung über die Gefahren der modernen Informationsgesellschaft notwendig sei.

3 Folgerungen für die Systemgestaltung

Eine Bewertung technischer Entwicklungen als wünschenswert bzw. nicht-wünschenswert setzt die Orientierung an einer Wertgrundlage voraus, die es im Rahmen einer wissenschaftlichen Arbeit dezidiert zu erörtern gilt. Der Rekurs auf faktische Akzeptanzlagen ist, wie bereits dargelegt, ein kaum gangbarer Weg (Irrationalität, Widersprüchlichkeit, Veränderlichkeit). Daraus abgeleitete Vorschläge der Systemgestaltung geraten zudem stark in die Nähe eines gefährlichen Seins-Sollens-Fehlschlusses, vor dem auch ausgereifte Studien nicht gefeit zu sein scheinen (vgl. z.B. [Bi06]). Die Erarbeitung einer allgemeingültigen, normativen Basis der Systembewertung erweist sich jedoch insofern als schwierig, weil angesichts des herrschenden moralischen und ethischen Pluralismus eine Vielzahl z.T. konfligierender Kandidaten zur Verfügung steht. Eine mögliche Lösung dieses Problems besteht darin, dass die unterschiedlichen ethischen Ansätze ihren Ausgangspunkt der Argumentation in der Freiheit des Menschen nehmen, jeweils unterschiedliche Facetten davon betonen, Freiheit jedoch selbst, auch als Grundgarant für Pluralismus überhaupt, nicht in Frage stellen (vgl. [Hu95], S. 113ff.). Die Bewertung der Akzeptabilität kontextsensitiver Systeme orientiert sich im Folgenden deshalb am Erhalt der Freiheit des Subjektes im Sinne des *Erhalts seines Handeln-Könnens* in Form der Sicherung basaler Vermächtnis- und Optionswerte (vgl. [Hu95], S. 129ff.). Aus dieser Perspektive erscheinen folgende Gestaltungsempfehlungen notwendig, um die Akzeptabilität der Systeme zu gewährleisten:
(1) Für den Nutzer sollte die Möglichkeit bestehen, auf die Systemnutzung verzichten zu können ohne von wesentlichen Entlastungseffekten und Serviceleistungen ausgeschlossen zu werden bzw. unzumutbare Einschränkungen zu erfahren. D.h.: Es sind technische Parallellösungen zu erhalten bzw. vorzusehen, die adäquate Ersatzleistungen ermöglichen, etwa der Art, dass eine sinnvolle Anzahl öffentlicher Telefonzellen vorgehalten wird, die auch das Telefonieren ohne die Nachteile der Mobiltelefonie in Form der detaillierten Erstellung von Bewegungsprofilen ermöglicht.

(2) Der sog. Janusköpfigkeit kontextsensitiver IuK-Systeme – also die prinzipielle Möglichkeit, dass spezifische Mittel immer auch unterschiedlichen Zwecken dienen können etwa durch Umwidmung von Datenbeständen – kann nur dadurch verhindert werden, dass Grenzen gesetzt werden, die nicht überwunden werden können. D.h.: Auf das Erheben von Daten ist in gewissen Bereichen zu verzichten (vgl. dazu auch den Beschluss des Oberverwaltungsgerichts Hamburg vom 22.11.2006 – 4 Bs 244/06, in dem einer softwaretechnischen Anonymisierung von Videobildern eine Absage erteilte wurde und stattdessen einen mechanische Blende für erforderlich gehalten wurde). Ist dies nicht möglich, ist der Aspekt der Zweckbindung und Datensparsamkeit unbedingt einzuhalten. Der Missbrauch bzw. die Kombination erfasster, heterogener Datenbestände ist durch Kurzzeitspeicherung, kryptographische Verfahren und Maßnahmen der Anonymisierung bzw. Pseudonomisierung von Nutzerdaten so weit wie möglich zu erschweren.

Während die ersten beiden Aspekte auf die prinzipielle Offenheit der Mittel-Zweck-Relation abheben (gleiche Zwecke können durch verschiedene technische Mittel erreicht werden; gleiche Mittel können unterschiedlichen Zwecken dienen), verweisen die folgenden Punkte eher auf den Erhalt und die Sicherung des Handeln-Könnens im Sinne eines selbstbestimmten Umgangs mit den Systemen:

(3) Revidierbarkeit ausgelöster Aktionen: Recht auf Möglichkeit der Löschung freigegebener persönlicher Daten und Informationen.

(4) Transparenz: Aufschluss über Art, Umfang, Weitergabe erfasster Daten; Informationen über das Systemverhalten und die Systemarchitektur.

(5) Vorhalten unterschiedlicher Nutzungsoptionen der Systeme: Im Spannungsfeld zwischen Zugriffsschutz und notwendigem Zugriff sind unterschiedliche Optionen der Nutzung bereitzuhalten (also nicht nur entweder/oder wie in Punkt (1)).

Letztendlich bleibt es jedoch ein Desiderat der Forschung, inwiefern bei der hohen Vernetzung und Komplexität ubiquitärer bzw. kontextsensitiver Systeme ein sinnvolles Maß an Systemtransparenz überhaupt (nutzerfreundlich) hergestellt werden kann bzw. inwiefern die notwendige Technisierung des Datenschutzes etwa durch Softwareagenten nicht selbst neue Intransparenzen und Unwägbarkeiten schafft. Auch gilt es ferner zu klären, inwiefern anonymisierte Daten aufgrund ihres hohen Detaillierungsgrades und Informationsreichtums trotzdem – oder gerade deswegen – dennoch eine Zuordnung zu spezifischen Personen ermöglichen bzw. inwiefern sichere kryptographische Verfahren aufgrund der niedrigen Rechenleistung ubiquitärer Systeme überhaupt möglich sind.

Literaturverzeichnis

[Bi06] Bizer, J. et al.: TAUCIS – Technikfolgenabschätzung ubiquitäres Computing und informationelle Selbstbestimmung, https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf, zuletzt abgerufen am 21.06.2007.

[Do99] DoCoMo: Vision 2010, http://www.nttdocomo.com/pr/1999/000868.html, abgerufen am 2007-06-28.

[Hu95] Hubig, Ch.: Technik- und Wissenschaftsethik. Ein Leitfaden. Springer, Berlin – Heidelberg – New York, 1995

[Is01] ISTAG: Scenarios for Ambient Intelligence in 2010. Compiled by Ducatel, K., et al. IPTS-Seville 2001, ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf, Abruf am 2007-06-28