

Ubiquitous Computing, Pervasive Computing, Ambient Intelligence ... Surveillance and Control?

Michael Nagenborg, Karsten Weber

BMBF-Projekt „Mobile Internetdienste und Privatsphäre“
Europa-Universität Viadrina Frankfurt (Oder)
Postfach 1786
15207 Frankfurt (Oder)
philosophie@michaelnagenborg.de
kweber@euv-frankfurt-o.de

Vorwort

Abstract: Sowohl im praktischen Diskurs von Bürgerrechtsvertretern und Datenschützern wie auch in theoretisch ausgerichteten Debatten werden Ausdrücke wie Ubiquitous Computing, Pervasive Computing und Ambient Intelligence meist negativ konnotiert. Dies hängt damit zusammen, dass diese Technologien der Überwachung (Surveillance) und Kontrolle (Control) dienen – wiederum zwei Ausdrücke, die meist im negativen Sinne als Freiheitsverlust oder gar Repression verstanden werden. Ziel des Workshops ist daher, sowohl theoretische Erwägungen als auch empirische Ergebnisse zusammenzuführen, um die Gründe für jene negative Konnotation aufzudecken und Wege zu ihrer Überwindung aufzuzeigen, wo dies geboten erscheint.

1 Der Workshop

Das Leitthema der INFORMATIK 2007 ist die Informatik bzw. die Produkte der Informatik als wichtige technische Voraussetzungen für moderne Logistik. Standen in diesem Zusammenhang bis vor kurzem vor allem die Verwaltung und Dokumentation von Warenströmen mithilfe von Computern und Datenbanken im Vordergrund – bspw. im Supply Chain Management (SCM) –, sind durch technische Entwicklungen, die zur Identifizierung von Gütern und zu ihrer exakten Lokalisierung im Raum genutzt werden können, ganz neue Möglichkeiten der informationstechnischen Unterstützung von Prozessen der Logistik möglich geworden. Stichwörter sind hier in erster Linie GPS (Global Positioning System) zur Lokalisierung und RFID (Radio Frequency Identification) zur berührungslosen Identifikation und Nahbereichslokalisierung. Solche Technologien können dazu genutzt werden, sowohl im Endkundengeschäft (B2C) als auch zwischen Unternehmen (B2B) neue Dienste anzubieten, so im Customer Relationship Management (CRM): Kunden können bspw. ständig über den genauen Stand von Lieferungen informiert werden, da diese in Raum und Zeit präzise geortet werden können. Dabei wachsen bspw. SCM und CRM zusammen bzw. greifen auf die gleichen Informationen zurück. Damit wird aber bereits auch ein problematischer Aspekt solcher Technologien

und Anwendungen angesprochen: Wer darf wann unter welchen Umständen auf welche Daten zurückgreifen?

In einem weiteren Sinne gehören solche Techniken wie RFID und GPS zu jenen, die schon eine Weile mit Ausdrücken wie Ubiquitous Computing, Pervasive Computing oder Ambient Intelligence (um der Kürze willen wird im Folgenden nur auf Ubiquitous Computing Bezug genommen) diskutiert werden bzw. können RFID und GPS als hierfür verwendbare Basistechnologien gedeutet werden. Mit Ubiquitous Computing sind nun Konzepte gemeint, die eine weitgehend vollständige Informatisierung der Lebens- und Umwelt implizieren. Nicht nur soll Rechenleistung in unbegrenzter Größe immer und überall zur Verfügung stehen, sondern unsere Lebens- und Umwelt soll unmittelbar auf unser Verhalten reagieren und verschiedenste Dienstleistungen bereitstellen. Die in diesem Zusammenhang häufig zitierten Beispiele sind, dass Wohnräume die anwesenden Personen identifizieren und die Umweltbedingungen an deren spezifische Bedürfnisse anpassen oder eine Verkehrssteuerung, die darauf beruht, dass jedes Objekt im Straßenverkehr exakt lokalisiert wird und sein Verhalten auf das anderer Objekte abgestimmt wird. Noch weiter gehen Ideen, die informationstechnische Artefakte in den menschlichen Körper integrieren wollen, um diesem einen direkten Zugang zu deren Leistungen zu ermöglichen.

Obwohl gerade die zuletzt genannten Ideen (noch) Zukunftsmusik darstellen und im Workshop keine explizite Rolle spielen, stellen Pläne, bspw. jedes einzelne Produkt in Supermärkten mit RFIDs eindeutig zu kennzeichnen, Vorstufen einer sehr weitgehenden Kolonisierung der Lebens- und Umwelt durch Informations- und Kommunikationstechnik dar. Wie so oft steht zu vermuten, dass eines Tages „neue Möglichkeiten“ dieser Technologien „entdeckt“ werden (function creep). Deshalb ist es auch nicht sonderlich überraschend, dass in vielen Diskussionen um solche Technologien insbesondere negative Konsequenzen eine große Rolle spielen – zumal in öffentlichen Debatten, die nicht selten fern technologischer Informiertheit geführt werden. Dabei wird Ubiquitous Computing meist in Zusammenhang mit Überwachung und Kontrolle der Bürger einer Gesellschaft gebracht – im Englischen meist mit dem Ausdruck „surveillance and control“ bezeichnet. Grundannahme des Workshops ist jedoch, dass diese Sichtweise zu eng ist, denn es sind Szenarien denkbar, in denen die entsprechenden Technologien so angewendet werden, dass dies sozial verträglich geschieht und mit bestehenden Bürgerrechten in Einklang steht.

Den Hintergrund des Workshops bildet die Forschungstätigkeit der Veranstalter im BMBF-Projekt „Mobile Internetdienste und Privatsphäre“, das von Karsten Weber geleitet wird. Michael Nagenborg ist zudem wissenschaftlicher Mitarbeiter in der Arbeitsgruppe von Rafael Capurro (HdM Stuttgart) im Rahmen des EU-Projektes „Ethicbots“.

2 Die Beiträge

Der Beitrag von *Ricarda Drüeke, Sonja Haug, Wolfgang Keller* und *Karsten Weber* bietet einen empirischen Zugang zu den genannten Fragen. Es werden Ergebnisse empirischer Studien vorgestellt, die aufzeigen, dass der Umgang mit Informations- und

Kommunikationstechnologie, die für Ubiquitous Computing genutzt werden kann, durch unterschiedliche soziologische Determinanten bestimmt wird. Interessant ist hierbei, dass selbst zwischen Menschen aus Ländern mit einer sehr ähnlichen Kultur deutliche Unterschiede in Hinsicht auf die Akzeptanz der Technologie zu beobachten ist und dass Datenschutz und Privatsphäre einen unterschiedlichen Stellenwert besitzen. Gerade für Unternehmen, die Produkte und Dienste grenzüberschreitend anbieten wollen, ist dies ein Hinweis, dass hierbei nicht nur im Marketing, sondern bei der Gestaltung von Produkten und Diensten selbst auf solche Unterschiede geachtet werden sollte.

Jens Gulden nähert sich dem Thema der Videoüberwachung aus einer bildphilosophischen Perspektive. Dabei betont er, dass diese bereits gängige Form der Überwachung in direkter Weise auf vorbegriffliche kognitive Operationen und somit die Grundlagen von Rationalität, formaler Symbolisierung und Abstraktion wirkt – und somit aus ethischer Perspektive abzulehnen sei. Er stellt damit einen kritischen Ansatz vor, dessen Anwendbarkeit auf andere Formen von Überwachung ebenso zu diskutieren sein wird wie die Frage nach „Eingriffstiefe“ von Ubiquitous Computing in die benannten Felder. Anders gefragt: Ist es möglich, ubiquitäre Systeme so zu entwerfen, dass sie die Kritik an der Videoüberwachung nicht trifft?

Im Beitrag von *Jessica Heesen* wird stärker der normative Bereich von Ubiquitous Computing angesprochen. Wie weiter oben schon angedeutet muss die Nutzung solcher Technologien nicht notwendig zu Konflikten mit Bürgerrechten führen. Stattdessen ist es denkbar, dass die Nutzung in einem normativen Rahmen stattfindet, der sowohl den Zwecken des Einsatzes gerecht wird als auch die Rechte der Nutzer und Betroffenen wahrt. Allerdings ist dies, wie Heesen aufzeigt, nur unter bestimmten, durchaus nicht-trivialen und gehaltvollen Bedingungen möglich – der so genannte „informed consent“ ist hierbei eine wichtige Voraussetzung, die aber gerade angesichts des ubiquitären Einsatzes von Informations- und Kommunikationstechnologie schwer zu erfüllen ist.

Martin Klamt zeigt wichtige theoretische Überlegungen zum Konzept des Raumes in Zusammenhang mit Ubiquitous Computing auf. Wenn in entsprechenden Debatten bspw. von öffentlichem oder privatem Raum die Rede ist, so kann damit nicht nur der physikalische Raum gemeint sein, bspw. die „eigenen vier Wände“, sondern muss immer auch die Funktion dieses Raums für Menschen mit in Rechnung gestellt werden – sprich: psychologische, sozialpsychologische und soziologische Aspekte mit in Betracht gezogen werden. Dies zeigt Klamt insbesondere am Beispiel der Videoüberwachung auf, da diese als Paradigma der Überwachung und Kontrolle des öffentlichen Raums verstanden werden kann.

Wie bereits oben bemerkt, wird Überwachung und Kontrolle meist negativ konnotiert. *Michael Nagenborg* geht in seinem Beitrag zunächst dem Unbehagen der Philosophie angesichts der Frage nach moralisch akzeptablen Formen der Überwachung nach, gerade weil sie im Widerspruch zu jener negativen Bedeutung stehen. Dazu knüpft er zunächst an den Begriff der „ethical surveillance infrastructures“ an, der zurzeit in verschiedenen philosophischen und sozialwissenschaftlichen Debatten kontrovers diskutiert wird. Am Beispiel der Ethik von Ernst Tugendhat zeigt Nagenborg dann, wie Ethik und Überwa-

chung in einander greifen können, ohne die daraus möglicherweise resultierenden Probleme zu vergessen.

Die Nutzung jeder Technologie bringt subjektiv empfundene Chancen und Risiken mit sich, die jedoch nicht notwendig den objektiven Gegebenheiten entsprechen müssen. Von der Unterscheidung subjektiver Einschätzungen und objektiver Bedingungen ausgehend bewertet *Oliver Siemoneit* Technologien wie Ubiquitous Computing. Diese Unterscheidung ist deshalb von erheblicher Bedeutung bspw. für die Technikfolgenabschätzung, weil subjektive Einschätzung sowohl übertrieben sein als auch zu kurz greifen können – wir können Gefahren sehen, wo objektiv keine gegeben sind, aber wir können Risiken subjektiv auch verkennen, obwohl sie objektiv gegeben sind. Daher werden Technologien faktisch akzeptiert (abgelehnt), obwohl möglicherweise keine rational begründbare Akzeptabilität (Ablehnbarkeit) vorliegt. Anhand dieser Unterscheidungen entwickelt Siemoneit Kriterien, die für eine rational begründbare Akzeptabilität gegeben sein müssen – und ergänzt mit dieser alternativen Herangehensweise die Perspektive, die auch bei Jessica Heesen eröffnet wird.

Mal implizit, mal explizit wurde bereits angedeutet, dass die Debatte um Ubiquitous Computing nicht selten durch fehlendes Wissen und subjektive Bedrohungsängste geprägt ist. *Stefan G. Weber*, *Sebastian Ries* und *Andreas Heinemann* zeigen in ihrem Beitrag auf, dass es in jedem Fall bei Einsatz von Ubiquitous Computing inhärente Tradeoffs gibt: Weil Ubiquitous Computing überall und jederzeit Informations- und Kommunikationsdienste realisieren soll, müssen dafür bestimmte Bedingungen erfüllt sein: Die Nutzerinnen und Nutzer müssen identifiziert, der Kontext berücksichtigt oder Kosten personen- und dienstbezogen abgerechnet werden. Dies bedeutet die Produktion, Speicherung und Verarbeitung sensibler Informationen über Personen. Weber, Ries und Heinemann klären in ihrem Beitrag, dass daher unvermeidbare Zielkonflikte beim Einsatz von Ubiquitous Computing entstehen.

Im Mittelpunkt des Beitrages von *Klaus Wieglerling* steht die Forderung nach der Implementierung einer kommunikativen Option über die Systemeinrichtung, Systemkommunikation sowie Systemintegration in ubiquitäre Systeme. Die so genannte „Parallelkommunikation“ soll die im Hintergrund agierende Systeme begleiten, um deren Funktionalität aus der Perspektive der Nutzung überprüfen zu können und dabei verschwundene Schnittstellen wieder sichtbar machen. Durch eine kritische Begleitung soll Vertrauen in ubiquitäre Systeme hergestellt werden, indem sowohl die Schwächen und Grenzen eines Systems als auch sein tatsächliches Vermögen sichtbar werden.

3 Fazit

Die Vielfalt der Themen, die im Workshop „Ubiquitous Computing, Pervasive Computing, Ambient Intelligence ... Surveillance and Control?“ angesprochen werden, zeigen, dass die Entwicklung und Implementierung von Technologie eben nicht nur im weitesten Sinne technische Fragen aufwirft, sondern Designentscheidungen beinhalten, die weitreichende soziale Konsequenzen nach sich ziehen. Das allein bedeutet jedoch nicht, dass deshalb eine gegebene Technologie bereits als sozial oder moralisch negativ bewert-

tet werden muss. Die Beiträge zeigen, dass ein sozial verträglicher Einsatz von Informations- und Kommunikationstechnologie wie Ubiquitous Computing denkbar, aber nicht zum Nulltarif zu haben ist. Zumindest gestalterisches Denken und die Bereitschaft, im Vorfeld des Einsatzes soziale und moralische Fragen in Rechnung zu stellen, müssen erbracht werden. Das ist zwar keine hinreichende, in jedem Fall aber eine notwendige Bedingung für das Gelingen eines entsprechenden Vorhabens.