LIFIS ONLINE [01.12.07]
www.leibniz-institut.de
ISSN 1864-6972

Gerhard Banse

Ubiquitäre Elektronik. Gesellschaftliche Aspekte

In einem Übersichtsbeitrag „Internet der Dinge – Auf dem Wege zur ubiquitären Elektronik“ geht Bernd Junghans abschließend auf gesellschaftliche Aspekte ein.[1] Zur Erinnerung sollen die wichtigsten Aussagen hier nochmals zitiert sein (Junghans 2007, S. 8):

- „Die gesellschaftlichen Aspekte berühren nicht nur juristische Probleme wie die Wertung von Entscheidungen, die im fließenden Verkehr von Fahrerassistenzsystemen getroffen werden, oder die komplexen Probleme der Telemedizin. Auch der Schutz der Privatsphäre stellt ein wesentliches Problem gesellschaftlicher Akzeptanz dar.“
- „Gravierende Auswirkungen einer erkennbar zunehmend allgemeinen Einführung der ubiquitären Elektronik sind jedoch aus der enormen Steigerung der Produktivität in nahezu allen Bereichen menschlicher Aktivitäten zu erwarten.“
- „Die große Herausforderung für die künftige Gesellschaft ergibt sich […] aus der Frage, wie mit dem Reichtum, dem Überfluss an allen denkbaren Gütern und Dienstleistungen umgegangen wird, wenn nur noch ein geringer Bruchteil der Bevölkerung in diesen Wertschöpfungsprozess einbezogen sein wird. Ein weiteres Auseinanderdriften in eine wohlhabende Oberschicht und eine verarmende Unterschicht kann nicht im Interesse der inneren und äußeren Stabilität der Gesellschaft sein.“

Damit ist das Spektrum der gesellschaftlichen Implikationen des sich abzeichnenden „Internet der Dinge“ erst angedeutet, denn dieses reicht sicherlich von unterschiedlichen (globalen) ökonomischen Effekten über (nationale) Exklusions-/Inklusions-Prozesse bis zu Einflüssen auf die (individuelle) Privatsphäre.[2] Daran anknüpfend sollen im Folgenden einige weitere Facetten verdeutlicht werden. Zu berücksichtigen ist dabei, dass viele gesellschaftliche Aspekte derzeit nur erahnt werden können, vielfach nur hypothetisch (etwa als Extrapolationen von oder Analogien zu Gegenwärtigem) vorhanden sind oder auch nur allgemein debattiert werden. Aber genau dieses ist z.B. das Anliegen von Technikfolgenabschätzung/Technikbewertung: Das *systematische, methodische* Analysieren und Bewerten von Voraussetzungen und Wirkungen technischer Hervorbringungen und technisch instrumentierten Handelns mit dem Ziel des Verdeutlichens unterschiedlicher Optionen für Zukünftiges (vgl. Banse/Lorenz 2007, S. 239ff.; vgl. auch BSI 2004, Hilty et al. 2003).

---

1 Dabei wird ausdrücklich die weitere Diskussion gesellschaftlicher Implikationen gefordert und dabei auf Banse/Lorenz 2006 verwiesen. Dieser Beitrag liegt den folgenden Darlegungen zu Grunde (vgl. auch Banse/Lorenz 2007).

2 Ein guter Überblick findet sich im Abschnitt „Implikationen“ in Mattern 2003 (S. 29ff.); vgl. auch Banse et al. 2007.

1.

Die konstatierte Allgegenwart von Sensor- und Computer-Netzwerken in unserer Umgebung (also die „ubiquitäre Elektronik“) bedeutet auch die Allgegenwart von Abhängigkeiten im positiven wie im negativen Sinne, d.h. hinsichtlich Chancen und Gefahren. Chancen und Gefahren sind indes keine technischen Kategorien, sondern soziale: Technik ragt in die Gesellschaft hinein,

- ökonomisch, da sie in Wertschöpfungs- und Verwertungsprozesse eingebunden ist,
- politisch, da es z.B. einen rechtlichen ‚Rahmen’ gibt, in dem Herstellung und Nutzung erfolgen,
- sozial, da sie Arbeitsprozesse, Kooperationsbeziehungen sowie Arbeits- und Freizeit beeinflusst,
- kulturell, da sie Handlungsmuster und -praxen verändern kann,
- individuell-mental, da menschliche Vorstellungen (Erwartungen, Hoffnungen, Ängste, Befürchtungen) auch einen technischen Bezug haben.

Auf der einen Seite steht somit der technische Fortschritt, der zunächst an innertechnischen Kriterien wie Effizienz, Neuheit, Zuverlässigkeit usw. gemessen wird. Auf der anderen Seite geht es um gesellschaftliche Entwicklung, die durch solche Kriterien wie Selbsterhaltung, Selbstbestimmung und Selbstverwirklichung oder – in einer anderen Terminologie – durch Sozialverträglichkeit und Umweltverträglichkeit gekennzeichnet ist. Zwischen beiden besteht – zumal in unserer stark technisierten (d.h. technikgestützten) und funktional ausdifferenzierten Zivilisation – eine Abhängigkeit, die jedoch nicht direkt bzw. linear-deterministisch, sondern nur über zahlreiche Zwischenstufen vermittelt ist. Es gilt deshalb, technikinduzierte Gefahren und Chancen zu verdeutlichen, um diese Chancen befördern, die Gefahren hingegen vermeiden, minimieren, kompensieren zu können

Deutlich wird: Unser gegenwärtiges Leben i.w.S. gründet sich weitgehend auf der (wissenschaftsbasierten) Entwicklung und umfassenden (teilweise exzessiven) Nutzung technischer Mittel (technischer Sachsysteme). Dieser „Vormarsch“ des „Gemachten“ in die Welt des „Gegebenen“ – um eine Charakterisierung von Günter Ropohl zu verwenden (vgl. Ropohl 1991, S. 20) – hat zahlreiche lebensweltlich aufweisbare Effekte vor allem sozialer, ökonomischer, politischer, kultureller und ökologischer Art; für jeden Menschen offensichtlich ist der Einfluss auf die gesamte Arbeits- und Lebensweise (vgl. Banse 1996, S. 252ff.). Folgerichtig wird dieser Prozess nun zunehmend von Diskussionen über seinen ‚Sinn’ oder ‚Unsinn’, sein Tempo und Ausmaß, seine Richtung(en) und Beeinflussbarkeit usw., von so genannten Technikdebatten begleitet (die – wie die obigen Beispiele zeigen – nicht nur technikkritisch verstanden werden dürfen!).

Diese Technikdebatten entzünden sich in der Regel vorrangig jedoch nicht an der (inneren) Funktion technischer Mittel, sondern *einerseits* an deren Ziel- bzw. Zwecksetzung, *andererseits* an deren (möglichen und wirklichen) Folgen, Wirkungen, Effekten usw. in individueller, ökonomischer, sozialer, ökologischer u.a. Hinsicht.

2.

Ein wichtiger, vor diesem Zusammenhang zu klärender *Ausgangspunkt* – auf den Junghans selbst verweist (vgl. Junghans 2007, S. 1) – ist das *Sicherheitsverständnis*, denn ‚Sicherheit’ ist ein fa-

cettenreicher, schillernder Begriff. In der interessanten Studie „Sicherheit als soziologisches und sozialpolitisches Problem“ hat der Soziologe Franz-Xaver Kaufmann Anfang der neunzehnhundertsiebziger Jahre 18 unterschiedliche Bedeutungen von Sicherheit ermittelt (vgl. Kaufmann 1973).

Im Deutschen wird ‚Sicherheit’ in mindestens drei Hauptbedeutungen verwendet:

1. Sicherheit als Geborgenheit,
2. Sicherheit als Selbstsicherheit,
3. Sicherheit als Systemsicherheit (herstellbare, berechenbare Mittel für beliebige Zwecke).

Alle drei Hauptbedeutungen betreffen auch diejenigen menschlichen Hervorbringungen, die das kennzeichnen, was mit ubiquitärer Elektronik bezeichnet wird (vgl. näher Banse 1998).

Sicherheit bedeutet

- (einerseits) die Abwesenheit bzw. den Ausschluss von Gefahren für Leib und Leben sowie
- (andererseits) solche Bedingungen, die die körperliche wie geistige Unversehrtheit, das Überleben und die Weiterentwicklung des einzelnen Menschen wie der ganzen Menschheit ermöglichen.

Gefahr bedeutet eine Lage, in der bei ungehindertem Ablauf des Geschehens ein Zustand oder ein Verhalten mit hinreichender Wahrscheinlichkeit zu einem Schaden für die genannten Schutzgüter der Sicherheit führen würde.

Vor diesem Hintergrund kann man Sicherheit

- als menschliches „Urbedürfnis“ (vgl. Bachmann 1991),
- als Menschenrecht (vgl. Robbers 1987),
- als Wertidee hochdifferenzierter Gesellschaften (vgl. Kaufmann 1973)

betrachten. Zugleich gilt es aber auch,

- ein „Menschenrecht auf Irrtum“ (vgl. Guggenberger 1987) im Umgang mit technischen Sachsystemen (auch solcher elektronischer Art) zu konstatieren sowie
- „Fehlerfreundlichkeit“ (vgl. u.a. Weizsäcker/Weizsäcker 1984; Wehner 1992) auch in diesem Bereich zu schaffen.

3.

Durch die genannte Allgegenwärtigkeit von Computern gewinnen im Zusammenhang mit der gerade charakterisierten Sicherheit vor allem (technische) Zuverlässigkeit sowie solche Bewertungskriterien wie Verfügbarkeit, Integrität und Vertraulichkeit an Bedeutung.

Zuverlässigkeit sei technisch als Maß der Funktionserfüllung eines technischen Sachsystems und seiner Elemente in Abhängigkeit von Alter, Belastung und Umgebungsbedingungen gefasst. Das schließt auch den Ausschluss von Übertragungsfehlern ein. Darauf sei hier nur verwiesen, etwa im Zusammenhang mit sensiblen Anwendungen (Medizin, Sicherheitstechnik, Umwelt- oder Bauwerkmonitoring), denn es gibt zahlreiche technische ‚Standard-Lösungen’ zu Erhöhung der Zuverlässigkeit.

Verfügbarkeit wird als Abwesenheit der Beeinträchtigung der Funktionalität des betreffenden Elektronik verstanden. Verfügbarkeit hat eine technische Seite (etwa im Zusammenhang mit der Zuverlässigkeit). Bedeutsam sind in diesem Zusammenhang indes ‚außertechnische' Einflüsse. Verfügbarkeit bedeutet dann etwa die Verhinderung einer unbefugten Beeinträchtigung der Funktionalität. Man denke nur daran, dass es derzeit u.a. in Flugzeugen, Krankenhäusern (noch) untersagt ist, Mobiltelefone zu benutzen. Oder man stelle sich vor, dass GPS gestört oder abgeschaltet wird …

Integrität schließlich bedeutet, dass die Messgrößen, Daten usw., die von ‚ubiquitärer Elektronik' (vor allem in Form von Sensorsystemen) ‚registriert' und evtl. weitergeleitet werden, weder ‚systemintern' noch ‚systemextern' (unbefugt) modifiziert oder gelöscht werden können. Man denke in diesem Zusammenhang nur an die Insulingabe, die bei bestimmten Systemen automatisch auf der Grundlage der Messung des Blutzucker-Gehalts erfolgt, an eine polizeiliche Blutalkohol- oder Geschwindigkeits-Kontrolle. Integrität der (technischen) Systeme im oben genannten Sinne ist dafür eine notwendige Bedingung.

Schließlich ist noch auf das Kriterium der *Vertraulichkeit* verwiesen, mit dem ausgedrückt wird, dass nur Berechtigte Zugriff auf die Messgrößen, Daten usw. eines Sensorsystems haben dürfen. Das ist bei Raumtemperaturangaben sehr wahrscheinlich weniger bedeutsam als etwa bei firmeninternen Daten. Eine in den gesellschaftlichen Entwicklungsbereich ragende Problematik beispielsweise ist die der rechtlichen Regelungen im Umfeld der Nutzung von Sensorsystemen. Wie sind etwa die Haftpflicht- oder Schadenersatz-Regelungen bei Ausfällen von Sensoren/Sensor-Netzen, etwa bei Fahr-Assistenz-Systemen, zu gestalten, wie bei Verlust von Verfügbarkeit, Integrität und Vertraulichkeit? Generell kann man immer auf die ‚letztendliche Zuständigkeit' der nutzenden Person, ihre Verantwortung verweisen. Ist das aber zukünftig ausreichend?

4.

Die Allgegenwart von Computern und Sensorsystemen verweist erneut auf die „Ironien der Automatisierung", darauf, dass sie – wenn manchmal auch sehr vermittelt – in Mensch-Technik-Systeme und -Interaktionen eingebunden sind. Mit den „Ironien der Automatisierung" hat Lisanne Bainbridge bereits 1987 darauf verwiesen, dass in der hochautomatisierten Industrie für menschliche Tätigkeiten die Voraussetzungen für eine zuverlässige (d.h. fehler- und irrtumsfreie) Tätigkeitsregulation oft nicht erfüllt sind (vgl. Bainbridge 1987):

1. Indem Automatisierung dem Menschen den leichten Teil seiner Aufgabe wegnimmt, kann sie den schwierigen Teil der Aufgabe eines menschlichen Operators noch schwerer machen.
2. Auch ein hoch automatisiertes System braucht Menschen zur Überwachung des Systems und um auf Störfälle zu reagieren.
3. Systemdesigner versuchen, den menschlichen Faktor als Fehlerquelle zu beseitigen. Doch (a) die Designer von Systemen sind auch Menschen und (b) lässt sich nicht alles automatisieren.
4. Diejenigen Teile eines Prozesses, von denen die Systemdesigner nicht wissen, wie sie automatisiert werden können, müssen weiterhin durch den Operator gesteuert werden.

Wendet man die gerade angestellten Überlegungen nicht nur auf einzelne Individuen oder soziale Gruppen, sondern auf die gesamte Gesellschaft an, dann führt das zu Überlegungen, die bereits im Jahre 1989 zur Rede von der „Verletzlichkeit der Informationsgesellschaft geführt hatten (vgl.

Roßnagel et al. 1989). Gemeint ist damit „die *Möglichkeit großer Schäden für die Gesellschaft*. Sie kann durch die (Informations- und Kommunikations-) IuK-Technik beeinflusst werden, indem sie das *Schadenspotential oder die Fehler- und Mißbrauchsmöglichkeiten technischer Systeme verändert*“ (Roßnagel et al. 1989, S. 9).

5.

Diese ‚Verletzlichkeit' von Gesellschaft und auch von Wirtschaft im Zusammenhang mit IuK-Technik, diese Herausbildung ‚kritischer Infrastrukturen' – um einen anderen Terminus zu verwenden – wird in Fällen von Computerpannen und -ausfällen, in technischen Störfällen und Havarien, in Sabotage-Akten und man-made-Katastrophen schlagartig sichtbar. Man denke etwa an Viren, Hacker, DoS-Attacken, Spam u. a..

Die Verfasser des genannten Buches hatten u.a. folgende Thesen aufgestellt (vgl. Roßnagel et al. 1989, S. 208ff.):

- Die Verletzlichkeit der Gesellschaft wird künftig ansteigen und zu einem zentralen Problem der Informationsgesellschaft werden.
- Die Struktur der Verletzlichkeit wird sich im tatsächlichen wie im Wissen gegenüber heute verändern.
- Das Sicherheitsniveau könnte sehr hoch sein, wird in der Praxis aber deutlich unter den theoretischen Möglichkeiten liegen.
- Zahl und Intensität der Missbrauchsmotive nehmen überproportional zu.
- Das Schadenspotenzial von IuK-Systemen wird deutlich zunehmen. Die Gesellschaft wird in nahezu allen Bereichen vom richtigen Funktionieren dieser Techniksysteme abhängig sein.
- Gesamtgesellschaftliche Katastrophen durch den Ausfall wichtiger sozialer Funktionen, die Techniksystemen übertragen wurden, sind nicht auszuschließen.

Gegenwärtige Ereignisse belegen die Weitsicht der Autoren. Allerdings kommen die von ihnen vor fast zwanzig Jahren formulierten Überlegungen gegenwärtig erst allmählich zum Tragen. Den Hintergrund dafür bilden:

- Immer mehr Bereiche in Wirtschaft, Verwaltung (Militär) und Politik sind nur noch dann arbeitsfähig, wenn die IuK-Technik sicher und zuverlässig funktioniert („neue Abhängigkeiten“), das betrifft (a) die Datenerstellung, (b) die Datenverwaltung und Datenspeicherung, (c) die Datenverarbeitung und (d) die Datenübertragung.
- Die ausgetauschten Informationsmengen wachsen exponentiell und explosionsartig.
- Die Globalisierung und Privatisierung (outsorcing) aller (vieler) Prozesse betrifft (a) auch informationelle Beziehungen und macht (b) vor organisatorischen bzw. staatlichen Grenzen keinen Halt (free flow of information).
- Die Forderung nach Schutz von persönlichen, firmeneigenen und regierungsamtlichen Daten wird immer stärker.
- Die Forderung nach sicherer Informations- und Kommunikationstechnik (informationstechnische Sicherheit: Zuverlässigkeit, Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität) nimmt zu.

Infolgedessen bilden sich immer mehr kritische Infrastrukturen heraus: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (BSI o.J.). „Kritische Infrastrukturen […] sind in vielen Wirtschaftssektoren, u.a. im Bank- und Finanzwesen, im Verkehrs- und Verteilungssektor, in den Bereichen Energie, Versorgungseinrichtungen, Gesundheit, Lebensmittelversorgung und Kommunikation sowie der wichtigen Dienste des Staates zu finden“ (EU 2004).

6.

Bei Fragen im Zusammenhang mit Privatheit – gegenwärtig vor allem als „individuelle Grundrechte contra staatliche Pflichten (zur Gefahrenabwehr)“ debattiert – handelt es sich um eine zentrale Thematik der Zivilgesellschaft:

Einerseits geht es um die Sicherstellung der (individuellen) Grundrechte (vor allem Schutz der Menschenwürde). Als Beispiel sei auf das Recht auf informationelle Selbstbestimmung verwiesen (vgl. auch EPTA 2006): In seinem „Volkszählungsurteil“ vom 15. Dezember 1983 hat das deutsche Bundesverfassungsgericht (BVerG) dieses informationelle Selbstbestimmungsrecht höchstrichterlich anerkannt: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine dies ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“ (BVerGE 65, 1, S. 43). Das bedeutet, das jede Person wissen können muss, wer was wann und bei welcher Gelegenheit über sie weiß, in Erfahrung bringen oder speichern kann.

Andererseits gibt es die staatliche Pflicht etwa zur Kriminalitäts- bzw. Terrorismusvorbeugung und -bekämpfung, d.h. zur Gefahrenabwehr und Schadensabwendung für die Bürger wie für das Gemeinwesen. Mittel dafür sind u.a. Videoüberwachungen, der „Große Lauschangriff“, das „Luftsicherheitsgesetz“, online-Computer-„Durchsuchungen“, die „Vorrats-Daten-Speicherung“, verdachtsunabhängige Rasterfahndung, Reisepässe mit biometrischen Daten u.a. (also fast durchweg IKT-gestützte Methoden). Als in dieser Hinsicht exzessive Beispiele sei nur auf die Fußball-WM 2006 in Deutschland oder den G8-Gipfel in Heiligendamm verwiesen. Trotz beschwichtigender Erklärungen der Verantwortlichen gilt: „Ich sage voraus, dass alles, was irgendwie technisch möglich ist, eines Tages unter diesem Druck, Sicherheit herzustellen, gemacht werden wird. […] Das heißt also, die technische Innovation wird benutzt, die Effizienz der inneren Sicherheit voranzutreiben. Das sind zum Teil ganz untaugliche Mittel, und es sind vor allen Dingen Mittel […], die ihre Grenze nicht dort finden, wo […] die Verfassung die Grenze sehen, nämlich beim Schutz der Menschenwürde. Nicht alles, was zum Erfolg der Strafverfolgung beitragen kann, darf gemacht werden“ (Baum 2006).[3]

3 Gerhart Baum war von 1972 bis 1978 Parlamentarischer Staatssekretär beim deutschen BMI und von 1978 bis 1982 deutscher BMI.

7.

Mit den oben hervorgehobenen Technikdebatten ist zugleich auf die Problematik der Technikakzeptanz und der Technikakzeptabilität verwiesen – Begriffen, die oftmals zu undifferenziert verwendet werden. Schon vor mehr als einem Jahrzehnt wurde auf drei unterschiedliche Ebenen von Akzeptanz-Überlegungen hingewiesen:

1. Verhalten gegenüber der Technik, wobei sich dieses auf konkrete technische Produkte, Verfahren und Systeme in bestimmten raumzeitlichen Zusammenhängen bezieht,
2. Einstellungen gegenüber dem Gesamtsystem Technik,
3. Komplexe sozio-kulturelle Sinnsysteme, in die die Technik ‚eingebettet' ist und in der sie eine mehr oder weniger prominente Rolle spielt (vgl. König 1993, S. 254).

Zugleich hat König überzeugend gezeigt – und dem ist zuzustimmen –, dass die Ebene 2 die problematischste hinsichtlich der Gewinnung ihrer Datenbasis und der Interpretation dieser Daten ist.

Weitergehend ist darauf zu verweisen, dass (Technik-)*Akzeptanz* das Ergebnis komplizierter, rational wie emotional vollzogener Wertungs- und Entscheidungsprozesse gegenüber technischen Sachsystemen und den Folgen ihrer Nutzung ist, bei denen die erwarteten Implikationen optionaler Handlungs- und Sachverhaltsarten individuell gewichtet und mit anderen Faktoren (vor allem gesellschaftlich-kulturellen) zu einem Gesamturteil verschmelzen. Es kommt zu einer Abwägung zwischen dem subjektiv gewichtetem angestrebten Nutzen und den möglichen Gefahren oder negativen Implikationen der technischen Handlung oder technologischen Lösung, die zu ihrer Akzeptanz (auch in Form einer Duldung) oder ihrer Ablehnung führt. (Technik-)Akzeptanz beschreibt somit faktisches Verhalten von Individuen oder Gruppen gegenüber Technik.

(Technik-)*Akzeptabilität* hingegen erfasst Normatives: Es handelt sich um ein normatives Urteil über die Zumutbarkeit der Nutzung einer technischen Lösung oder eines technischen Sachsystems, also um eine (hypothetische?) Aussage, ob und unter welchen Bedingungen eine bestimmte Technik akzeptiert werden würde. Diese Aussage beruht immer auf subjektiven Wertungen – auch dann, wenn formale Entscheidungsverfahren angewendet werden –, in die auch Emotionales (in Wechselwirkung mit Rationalem) eingeht. Aussagen über Akzeptabilität beziehen sich immer auf einen vorgängigen Maßstab, etwa hinsichtlich Sozial-, Umwelt-, Verfassungs- oder Humanverträglichkeit.

Eigentlich sind es nur sehr wenige konkrete Technologien bzw. deren spezielle Anwendungsbereiche, die der Öffentlichkeit (bzw. eines Teils von ihr) Sorge bereiten (z.B. nukleare Energieerzeugung, Gentechnik in Landwirtschaft und Nahrungsmittelproduktion, s.o.). Auf der anderen Seite stellen die Informations- und Informationstechnologien einen Bereich dar, der (zumindest in bestimmten Segmenten der Bevölkerung) weitgehend unkritisch und vielfältig genutzt wird, obwohl er – wie vorstehend gezeigt wurde – Anlass zu kritischer Befragung bietet.

8.

Abschließend muss ein Gedanke von Bernd Junghans etwas differenzierend-weiterführend aufgegriffen werden. Wenn er schreibt, „Alle Erfahrungen aus der Geschichte belegen, dass sich produktivitätssteigernde Mittel und Verfahren unaufhaltsam und gegen alle Widerstände durchsetzen" (Junghans 2007, S. 8), so wird damit eine technikdeterministische und fatalistische Sichtweise zumindest nahegelegt. Allein die Fülle technischer Erfindungen, die sich nicht durchgesetzt

haben (oder anders ausgedrückt, die keine Innovation geworden sind) und die viele Museumssäle füllen, belegen, dass die gesellschaftliche Diffusion und Durchsetzung technischer Neuerungen alles andere als ein automatischer Prozesse ist. Dazu sei lediglich eine Anmerkung gemacht: Unter der Voraussetzung, dass eine Neuerung in der Lage ist, ein (latentes oder akutes) Bedürfnis befriedigen zu können, ist im Verlaufe ihrer praktischen ‚Umsetzung' – nach Rudolf Reichel – zumindest eine ethisch-soziologische, eine ökonomische und eine Ressourcenschwelle (vgl. Reichel 1981), nach Diethard Schade die Wissens-, die Methoden-, die Kommunikations- und die Machtbarriere (vgl. Schade 1991, S. 25ff.) auch (aber nicht nur und evtl. nicht vorrangig) durch den Einsatz der „geistigen Urheber" zu überwinden.[4] Der Erfolg, die ‚Karriere' bestimmter technischer Entwicklung hängt somit vom Vorhandensein vielfältiger Randbedingungen ab! Trotz dieser Einschränkung ist folgender Aussage von Bernd Junghans uneingeschränkt zuzustimmen: „Es ist an der Gesellschaft, die Folgen derartiger Entwicklungen rechtzeitig zu erkennen und darauf zu reagieren" (Junghans 2007, S. 8).

Literatur

Bachmann, Ch. (1991): Sicherheit. Ein Urbedürfnis als Herausforderung an die Technik. Basel/ Boston/Berlin

Bainbridge, L. (1987): Ironies of Automation. In: Rasmussen, J.; Duncan, K.; Leplat, J. (eds.): New Technology and Human Error. Chichester a. o., pp. 271-283

Banse, G. (1996): „Technizismus oder Humanismus?" – Philosophische Reflexionen über eine notwendige Debatte, die, weil sie nie geführt wurde, zum Stolperstein werden kann –. In: Tauss, J.; Kollbeck, J.; Mönikes, J. (Hg.): Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik. Baden-Baden, S. 248-269

Banse, G. (1998): Sicherheit zwischen Faktizität und Hypothetizität. In: Forum der Forschung. Wissenschaftsmagazin der Brandenburgischen Technischen Universität Cottbus, H. 6, S. 34-39

Banse, G.; Grunwald, A.; Hronszky, I.; Nelson, G. (eds.) (2007): Assessing Societal Implications of Converging Technological Development. Berlin

Banse, G.; Lorenz, C. (2006): „Sensornetze im Spannungsfeld zwischen technischem Fortschritt und gesellschaftlicher Entwicklung"; 3rd Leibniz Conference of Advanced Science, 2006. – URL: http://www.leibniz-institut.de/cms/pdf/Banse-Lorenz-Sensornetze_im_Spannungsfeld.pdf

Banse, G.; Lorenz, C. (2007): Technikfolgenabschätzung und „Ubiquitous Computing". Sensosysteme im Spannungsfeld zwischen technischem Fortschritt und gesellschaftlicher Entwicklung. In: Wangermann, G. (Hg.): Theoria cum praxi. Fünf Jahre Leibniz-Institut für interdisziplinäre Studien e. V. (LIFIS). Berlin, S. 237-256 (Sitzungsberichte der Leibniz-Sozietät, Bd. 90)

4 Wie die Geschichte der Technik vor allem in Form des Patentwesens und des Innovationsgeschehens verdeutlicht, wäre es ein Fehler anzunehmen, dass mit dem Einsatz aller persönlichen, organisatorischen und materiellen Mittel der Erfolg, d.h. die Durchsetzung einer technischen Neuerung, gesichert sei; erforderlich sind auch – wie bereits betont – entsprechende „Umwelt"bedingungen, die vom Erfinder oder Konstrukteur nicht bzw. nur bedingt beeinflusst werden können.

Baum (2006): Interview mit Gerhart Baum – „10 Jahre Grundrechte-Report". In: Neue Rheinische Zeitung, 14.06.2006. – URL: http://www.nrhz.de [16.05.2007]

BSI – Bundesamt für Sicherheit in der Informationstechnik (o.J.). – URL: http://www.bsi.de/fachthem/kritis/index.htm [16.05.2007]

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hg.) (2004): Risiken und Chancen des Einsatzes von RFID-Systemen. Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Ingelheim

EU (2004): Mitteilung der EU-Kommission „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung. – URL: http://www.euractiv.com/de/sicherheit/kritische Infrastrukturen/... [16.05.2007]

Guggenberger, B. (1987): Das Menschenrecht auf Irrtum. Anleitung zur Unvollkommenheit. München/Wien

Hilty, L.; Behrendt, S.; Binswanger, M.; Bruinink, A.; Erdmann, L.; Fröhlich, J.; Köhler, A.; Kuster, N.; Som, C.; Würtenberger, F. (2003): Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Bern (TA-SWISS)

Junghans, B. (2007): Internet der Dinge – Auf dem Wege zur ubiquitären Elektronik. In: LIFIS ONLINE – ISSN 1864-6972 (B. Junghans [14.08.07]). – URL: www.leibniz-institut.de

Kaufmann, F.-X. (1973): Sicherheit als soziologisches und sozialpolitisches System. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften. 2. Aufl. Stuttgart

König, W. (1993): Technikakzeptanz in Geschichte und Gegenwart. In: König, W.; Landsch, M. (Hg.): Kultur und Technik. Zu ihrer Theorie und Praxis in der modernen Lebenswelt. Frankfurt am Main u. a., S. 253-275

Mattern, F. (2003): Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Mattern, F. (Hg.): Total vernetzt. Szenarien einer informatisierten Welt. Berlin/Heidelberg, S. 1-41

Reichel, R. (1981): Zu einigen Entstehungsbedingungen und Gesetzmäßigkeiten der Ausbreitung komplexer Neuerungsprozesse in der Volkswirtschaft. In: Mitteilungen zu wissenschaftsökonomischen Untersuchungen der Hochschule für Ökonomie Berlin, Heft 1/1981

Robbers, G. (1987): Sicherheit als Menschenrecht. Aspekte der Geschichte, Begründung und Wirkung einer Grundrechtsfunktion. Baden-Baden

Ropohl, G. (1991): Einleitung in die Technikphilosophie. In: Ropohl, G.: Technologische Aufklärung. Beiträge zur Technikphilosophie. Frankfurt am Main, S. 11-30

Roßnagel, A.; Wedde, P.; Hammer, V.; Pordesch, U. (1989): Die Verletzlichkeit der „Informationsgesellschaft". Opladen

Schade, D. (1991): Technikbewertung und Produktfolgenabschätzung: Möglichkeiten und Grenzen. In: VDI (Hg.): Integrierter Umweltschutz. Ingenieurkonzepte für eine umweltverträgliche Technikgestaltung. Düsseldorf, S. 17-29

Weizsäcker, Ch.: Weizsäcker, E. U. von (1984): Fehlerfreundlichkeit. In: Kornwachs, K. (Hg.): Offenheit – Zeitlichkeit – Komplexität. Zur Theorie der Offenen Systeme. Frankfurt am Main/New York, S. 167-201

Wehner, Th. (Hg.) (1992): Sicherheit als Fehlerfreundlichkeit. Arbeits- und sozialpsychologische Befunde für eine kritische Technikbewertung. Opladen

[01.12.07]

Anschrift des Autors:

Prof. Dr. Gerhard Banse
Forschungszentrum Karlsruhe GmbH
Institut für Technologiefolgenabschätzung und Systemanalyse
Herrmann-von-Helmholtz-Platz 1
D – 76344 Eggenstein-Leopoldshafen