

## Das Internet der Dinge

Gesellschaftliche Herausforderungen der elektronischen Welt von morgen

aus: Vorgänge 184 ( Heft 4/2008), S.39-47

### I. Einleitung

Als 1993 mit dem World Wide Web das Internet publik wurde, war dies der Startschuss für eine neue Zeit. Eine Zeit, in der sich die Geschwindigkeit und das Ausmaß von Kommunikation und Informationsverteilung um ein Vielfaches potenziert hat im Vergleich zu dem, was Menschen noch in den 80er Jahren des 20. Jahrhunderts für ‚normal‘ hielten. Über Computer war (und ist) es plötzlich möglich, überall Informationen zu bekommen und selbst zu verteilen. Heute, in 2008, verfügen 58 Prozent aller Haushalte über einen Breitbandanschluss an das Internet[1]. Kaum ein Berufsbild der Wissensgesellschaft und kaum ein Privatleben scheinen mehr denkbar ohne das digitale Medium.

Etwa zur selben Zeit entstand noch ein zweites Phänomen: die Verbreitung von Mobiltelefonie. Schätzte man 1992 bei der Einführung der D-Netze noch hoffnungsvoll, dass vielleicht einmal 10 Millionen Kunden in Deutschland gewonnen werden könnten, so zählen wir heute über 100 Millionen Mobilfunkanschlüsse. Die Folge war (und ist) eine dramatische Steigerung der Mobilität und Flexibilität in der Organisation von Berufs- und Privatleben.

Doch wie gehen diese Entwicklungen weiter? Ist mit der gegenwärtigen Verfügbarkeit und Mobilität digitaler Dienste bereits ein Höhepunkt der Entwicklung erreicht, so dass man von zukünftigen Innovationen in diesem Bereich eigentlich nur noch abnehmende Grenznutzen erwarten darf? Was erwarten Wissenschaft und Forschung als die nächsten Schritte in dieser „digitalen Historie“? Wenn diese Frage gestellt wird, dann antworten Experten heute mit dem Begriff vom „Internet der Dinge“ als dem nächsten großen Innovationsschub.

Das Internet der Dinge verbindet und integriert die beiden Dimensionen der Verfügbarkeit und der Mobilität digitaler Dienste. Es wird begrifflich an vielen Stellen gleichgesetzt mit dem sog. „pervasive“ oder „ubiquitous computing“. Zu Deutsch, dem „allgegenwärtigen Rechnen“. Die Vision ist, dass nicht nur Computer und Mobiltelefone ein digitales Eigenleben und eine virtuelle Repräsentanz haben, die uns erlauben, durch sie zu kommunizieren, sondern dass in Zukunft alle Objekte über solche digitalen Eigenschaften verfügen. Dadurch soll der klassische Computer seine Bedeutung verlieren. Seine Funktionalität soll in die uns umgebenden Alltagsgegenstände eingehen. Der Urvater dieser Vision, Mark Weiser schreibt (1991): „The most profound technologies are those that disappear. *They weave themselves into the fabric of everyday life until they are indistinguishable from it.*“

Im vorliegenden Artikel soll nun diskutiert werden, welche sozialen Auswirkungen das Internet der Dinge haben könnte. Welche gesellschaftlichen Fragestellungen durch die neuen Technologien entstehen? Welche Fragen sollte man pro-aktiv stellen, um nicht blind in eine Welt digitaler Allgegenwärtigkeit zu laufen?

Die Gedanken und Erkenntnisse der folgenden Abschnitte wurden im Rahmen einer Technikfolgenabschätzung für das Ubiquitäre Computing gewonnen, die im Auftrag des BMBF von 2005 bis 2006 an der Humboldt-Universität zu Berlin in Kooperation mit dem Unabhängigen Landeszentrum für

Datenschutz in Schleswig-Holstein durchgeführt wurde[2] Der Begriff vom Internet der Dinge wurde hier gleichgesetzt mit dem des Ubiquitous Computing. Ferner wurde berücksichtigt, dass schon heute eine Vielzahl von digitalen Diensten vermarktet und genutzt werden, die sich in die langfristige Vision des Begriffs einordnen lassen.

## II. Soziale Fragestellungen in einer digitalen Welt von Morgen

Bei der Diskussion sozialer Faktoren im Zusammenhang mit elektronischen Systemen wird heute sehr häufig auf den Aspekt des Datenschutzes fokussiert. Datenschutzbedenken führen, so wird an vielen Stellen argumentiert, dazu, dass viele Konsumenten auf den elektronischen Handel (E-Commerce) verzichten. Zunehmend werden Menschen in ihrer Rolle als Kunden und Bürger durch Vorfälle des Identitätsdiebstahls und „Datenklau“ verunsichert.

Im Hinblick auf das Ubiquitous Computing geht man davon aus, dass sich diese Ängste der Menschen vor einem Missbrauch der Technik zurecht verschlimmern. Werden digitale Funktionalitäten in jeden erdenklichen Alltagsgegenstand integriert, so multipliziert sich auch die Anzahl der Schnittstellen zwischen Menschen und der digitalen Welt. Die Menge der über sie verfügbaren Daten und Informationen steigt stark an. Einige Wissenschaftler weisen daher schon heute darauf hin, dass das Internet der Dinge das Potenzial hat, traditionelle Modelle des Datenschutzes auszuhebeln: *„The most fundamental rules violated by ubiquitous information systems are the Collection Limitation Principle, the Purpose Specification Principle and the Use Limitation Principle” (Cas, 2005, S.24-33)*

Allerdings werden die sozialen Auswirkungen des Ubiquitous Computing in den gegenwärtigen Diskussionen in Presse und Wissenschaft gerne ausschließlich auf das Problem der Einbusse von Privatheit und Datenschutz reduziert. Dabei steht die Rolle des Menschen als Konsument oder Bürger im Vordergrund.

Soziale Auswirkungen des Ubiquitous Computing sollten jedoch auf einer breiteren Basis diskutiert werden und die unterschiedlichsten Rollen und gesellschaftlichen Austauschbeziehungen mit einschließen, in denen Technologie zum Einsatz kommt. Ferner sollte nicht nur die *informationelle* Selbstbestimmung betrachtet werden, wenn Ubiquitous Computing diskutiert wird, sondern es sollten auch die möglichen Folgen der Technologie(en) auf die *physische* Selbstbestimmung betrachtet werden.

Die folgenden Abschnitte beschäftigen sich daher zunächst mit einer erweiterten Betrachtung, wie der Einsatz von UC Technologie heute und in Zukunft Menschen in ihren unterschiedlichen Rollen tangieren. Der Artikel geht dann ein auf die Frage, wie die Privatsphäre im Sinne der informationellen aber auch physischen Selbstbestimmung durch UC Technologie berührt werden wird.

### II.1. Unterschiedliche Rollen von Menschen im Umgang mit Technologie

Um das gesamte Spektrum aufzuspannen, in dem informationelle Selbstbestimmung im Ubiquitous Computing betrachtet werden sollte, bietet sich das Pyramidenmodell von Parasuraman an (Parasuraman, 2000). Hier wird Technologie im Zentrum eines Spannungsfeldes zwischen Unternehmung, Arbeitnehmer und Konsument gesehen. Der Arbeitnehmer steht mit seinem Arbeitgeber in einer internen Beziehung, welche von Technologie beeinflusst wird (z.B. E-Mail, Mobiltelefonie, GPS, RFID, Batch-Systeme). Gleichzeitig steht der Arbeitnehmer in einer Beziehung zum Kunden der Unternehmung und nutzt

Technologie, um diese Beziehung zu optimieren (z.B. durch Customer Relationship Management Software). Und schließlich steht die Unternehmung direkt in Beziehung zum Kunden, wenn sie die Kanäle zum Kunden nutzt, die ihr mittels moderner Technologie zur Verfügung stehen (z.B. elektronische Nachrichten, automatisiertes Ticketing).

Soziale Auswirkungen von Ubiquitous Computing sind auf all diesen Beziehungsebenen greifbar. So kam es z.B. zu einem Aufstand von Lastwagenfahrern einer Speditionsgesellschaft, als diese mittels moderner Ortungstechnik prüfen wollte, wo genau sich ihre Fahrer befinden und wie viel Zeit sie auf welchen Streckenabschnitten verbringen. Dieses Anwendungsbeispiel ist nur eines unter vielen, welches die Frage aufwirft, wie stark Unternehmen ihre Mitarbeiter mit Technologie überwachen dürfen. Es gibt aber auch noch andere Faktoren, wo Technologie die Beziehung zwischen Arbeitnehmer und Arbeitgeber prägt: z.B. etablieren sich Erwartungshaltungen auf Seiten des Arbeitgebers, was Erreichbarkeit und Antwortzeiten angeht oder die aktive Nutzung multipler Endgeräte und Softwarelösungen (nicht nur E-Mail und Telefon, sondern auch Instant Messaging, Webcam, Beeper, Groupware, Blackberries, etc.).

Je nachdem, wie Arbeitgeber Technik im Arbeitsumfeld einsetzen, können sich also in unterschiedlicher Form soziale Konsequenzen aus dem Ubiquitous Computing ergeben. Diese sind sicherlich an vielen Stellen positiv zu beurteilen. Zum Beispiel, wenn es möglich wird, dass Arbeitnehmer, ihre Arbeit flexibler gestalten, vielleicht sogar teil-weise von zu Hause arbeiten können und Wegezeiten sparen. An anderer Stelle muss je-doch ein Konsens gefunden werden, in wie weit durch die Technologie ermöglichte Erreichbarkeits-, Einsatz- und Überwachungsziele im Verhältnis zwischen Arbeitnehmer und Unternehmung sinnvoll sind.

Arbeitnehmer stehen darüber hinaus zunehmend in einer interaktiven Beziehung zu Kunden. Digital verfügbare Information erlaubt es Unternehmen heute, sehr viel mehr Wissen über bestehende oder zukünftige Kunden zu gewinnen. Dadurch kann ein Kundendialog gezielter erfolgen. Unternehmen haben die Möglichkeit Produkte und Services anzubieten, die auf Kundenbedürfnisse besser zugeschnitten sind. Allerdings führt die Personalisierung von Dienstleistungen auch dazu, dass die Kundenansprache nicht mehr einheitlich ist. Die von Kunden nicht kontrollierbare Kategorisierung (z.B. mit Hilfe von Scoring-Verfahren) wird von vielen Datenschützern kritisiert.

Die Ansprache von Kunden durch Unternehmen beinhaltet jedoch noch eine weitere Herausforderung, denn UC Technologie führt zu einer Multiplikation der potenziellen Informationskanäle und Kommunikationsschnittstellen mit Kunden. Aus sozialer Sicht stellt sich die Frage, in welchem Ausmaß und in welcher Form diese Informationskanäle von Unternehmungen frei genutzt werden sollen und dürfen. Wie soll man gesellschaftlich mit dem knappen Gut der menschlichen Aufmerksamkeit umgehen? Wie soll beispielsweise ein Kunde im öffentlichen Raum zukünftig angesprochen werden (z.B. durch interaktive Werbeplakate)? Welche Geschäftsmodelle sind ethisch akzeptable? Bis zu welchem Grad soll die Ansprache von Kunden automatisiert werden dürfen? Erste politische Debatten zeigen schon heute, dass Unternehmen nicht mehr das Recht gegeben wird, Kunden ungefragt telefonisch zu kontaktieren.[3] Aber welche Schnittstellen sollten für das interaktive Marketing generell genutzt werden dürfen? Und sollten Kunden umgekehrt das Recht auf eine „Mindestansprache“ bei Unternehmen haben?

## **II.2. Privatsphäre und informationelle Selbstbestimmung im Internet der Dinge**

Der Erhalt von Privatsphäre (als Ziel des Datenschutzes) spielt nach Meinung von Soziologen, eine wichtige Rolle in der Gestaltung zwischenmenschlicher Interaktion, menschlicher Weiterentwicklung und im Erhalt von Demokratie. In Deutschland spie-gelt sich das Streben nach dem Erhalt von Privatsphäre rechtlich im Begriff der "informationellen Selbstbestimmung" wieder, welches im Rahmen des Volkszählungsurteils

1982 aus Art. 1 des deutschen Grundgesetzes zur Menschenwürde abgeleitet wurde.

Soziologisch wird der Prozess, mit dem Menschen ihre Privatsphäre schützen oder aufgeben, als eine Art „Grenzverwaltung“ verstanden: „*Privacy is an interpersonal boundarycontrol process, which paces and regulates interaction with others*“, schreibt Erwin Altman, einer der Urväter der Privacy-Forschung 1975. Diese Grenzkontrollmechanismen können unterschiedlicher Natur sein. So unterscheiden Bohn et al. (2004) im Hinblick auf das Ubiquitous Computing zwischen vier Mechanismen, denen sich der Mensch als Individuum und als Teil eines gesellschaftlichen Systems bedient, um seine Privatsphäre zu erhalten:

### 1. natürliche (physische) Abschottung

---

- Vergessen
- Vergänglichkeit
- soziale Separierung von Information

Die physische Abschottung, wie etwas das Aufsuchen von einsamen Orten, scheint die am nächsten liegende Form des Schutzes der Privatsphäre zu sein. Jedoch spielt auch das Vergessen und die Vergänglichkeit von Informationen zur eigenen Person eine Rolle. Wenn wir anderen etwas anvertrauen oder auch schon mal Dinge sagen, die wir nicht wirklich meinen, gehen wir davon aus, dass andere diese Dinge vergessen und uns nicht nachtragen. Wenn dem nicht so ist, und Information weiter getragen wird, fühlen wir uns u.U. in unserer Privatsphäre verletzt. Ebenso spekulieren wir auf Vergänglichkeit von Informationen. Äußerungen (oft sogar Handlungen!) in unserer Jugend wollen wir uns nicht über Jahrzehnte nachtragen lassen. Werden uns Dinge, wie z.B. die Zugehörigkeit zu einer radikalen Fußballfangruppe in unseren 20ern, auch nach Jahrzehnten noch vorgehalten oder sogar sanktioniert, fühlen wir uns in unserer Privatsphäre verletzt, da uns auf Basis der Vergangenheit etwas suggeriert wird, was wir mit uns in unserer Gegenwart nicht mehr verbinden. Und schließlich die soziale Separierung von Information: hier gehen wir davon aus, dass unser Handeln in einem sozialen Kontext nicht (fälschlicherweise) auf einen anderen Kontext übertragen wird. Wenn jemand bei-spielsweise zu einer Prostituierten geht, erwartet er, dass diese Information im Bordellmilieu verbleibt und nicht seinen Arbeitgeber erreicht. Ebenso verhält es sich mit Informationen zu Krankheiten oder ausgefallenen Hobbies, die einen in eine ‚Schublade‘ schieben könnten, die man für sich selbst nicht anerkennt oder nicht kommunizieren möchte.

Bohn et al. (2004) zeigen auf, wie diese vier Grenzmechanismen durch Ubiquitous Computing Technologien außer Kraft gesetzt werden könnten. Durch Ortungstechnologien, Videokameras und generell eine Umgebung, die sich des Menschen „bewusst“ ist und auf diesen reagiert, wird es immer schwieriger sein, sich physisch abzuschotten. Arbeiten von Boyle (2003) und Adams (2000) zu geteilten Multimedia-Umgebungen verdeutlichen dies: wenn Mitarbeiter von zu Hause arbeiten und dabei Videokameras einsetzen, die den Kollegen verraten, wo sie sind und was sie machen, ist eine Abschottung im heimischen Arbeitszimmer nicht mehr so einfach möglich. Vor allem dann nicht, wenn Firmenrichtlinien eine aktive Kamera vorsehen. Ebenso ist es bei einem breiten Einsatz von Ortungstechnologie (wie GSM oder GPS) kaum noch möglich, den eigenen Aufenthaltsort zu verbergen, wenn diese zum Zwecke des Flottenmanagements (im Unternehmen) oder Auffinden von Freunden und Kindern eingesetzt werden; insbesondere dann nicht, wenn Arbeitgeber, Freunde oder Eltern erwarten, dass man die eigene Position regelmäßig offen legt.

Vergessen und Vergänglichkeit sind Eigenschaften von Menschen, nicht aber von Datenverarbeitungssystemen. Ist es uns möglich durch Ortungstechniken, RFID oder Sensoren, menschliche Bewegungsprofile, soziale Netze, Gesundheitszustände, Fahrverhalten etc. ständig aufzuzeichnen (z.B. zum Zwecke der Erbringung bestimmter Dienstleistungen), dann liegt auch das längerfristige Speichern und Auswerten solcher Information nahe (sofern dies datenschutzrechtlich erlaubt ist). So ist z.B. offen, wie ein

heute aktiver Fußballhooligan, der einmal in der Datenbank „Gewalttäter Sport“ gelandet ist, dort in den nächsten Jahrzehnten wieder gestrichen werden kann. Im Zweifelsfall wird er vielleicht auch als braver Familienvater in 20 Jahren noch auf die Teilnahme an Fußballspielen verzichten müssen.

Und schließlich soziale Separierung von Information: bei diesem Aspekt der Privatsphäre steht die Verwendung von Information im richtigen Kontext im Mittelpunkt der Betrachtung. Ein Fax oder Ausdruck darf nur von dem gelesen werden, für den es bestimmt ist. Ein Einblick ins Telefonierverhalten nur von dem genommen werden, der die Rechnung stellt. Häufig kommt es jedoch auch heute schon zu einem unkontrollierten Kombinieren von Informationen über Kontexte und „Berechtigte“ hinweg: sei es, dass der Kunde durch Überlesen des „Kleingedruckten“ in eine Vielzahl von Datenverarbeitungsprozessen eingewilligt hat oder dass die Verknüpfung von Informationen grundsätzlich erlaubt ist. So können Daten zweckentfremdet werden. Wie eine zweck-entfremdete Weiternutzung von Daten im UC verhindert werden soll, wo gerade diese Dienste auf eine Vielzahl von Informationen angewiesen sind, ist völlig ungeklärt.

Durch das Internet der Dinge wird es zu einer Potenzierung der Sammlung und Verarbeitung persönlicher Daten kommen. Die Frage, die sich nun stellt ist, ob diese Entwicklung von Bürgern als Bedrohung wahrgenommen wird, wie diese zu informationsintensiven Diensten stehen, in wie weit sie auf das Vorhandensein von „schützenden“

Gesetzen vertrauen und unter welchen Bedingungen sie der Datenverarbeitung zustimmen. Da wir uns noch in einem evolutorischen Frühstadium bei der Entwicklung der digitalen Welt befinden, sind Antworten auf diese Fragen einem dauernden Wechsel unterworfen. Was heute noch als zutiefst private und intime Information gewertet wird, kann schon morgen als „common knowledge“ angesehen werden. Millionen von Deutschen tummeln sich heute in sozialen Netzwerken, wo sie freiwillig höchst genauen Einblick in ihr persönliches Profil geben, während Anfang der 80er Jahre noch im Rahmen des Volkszählungsurteils über die Preisgabe weniger Personenangaben gestritten wurde. Die Frage ist, ob man darüber urteilen darf, wer im Hinblick auf die digitale Welt von morgen „weiser“ ist: die Erstreiter des deutschen Datenschutzes, die auch in einer Welt des Ubiquitous Computing die Prinzipien der Datensparsamkeit und Zweckbindung nicht aufgeben wollen. Oder die möglicherweise überliberalen Technikfreunde der Zukunft, wie Scott McNeal, die sich mit Aussagen wie „*Privacy is dead, deal with it.*“ bekannt machen.

### II.3 Physische Selbstbestimmung im Ubiquitous Computing

Wie oben beschrieben gibt es neben der informationellen Selbstbestimmung im Internet der Dinge noch eine zweite und mindestens ebenso wichtige Herausforderung, nämlich die des Erhalts der physischen Selbstbestimmung des Menschen in intelligenten Umgebungen. Im Kern geht es dabei um die Kontrolle des Menschen über seine Objekte, wenn diese mit intelligenter Reaktionsfähigkeit ausgestattet werden bzw. autonom und im Hintergrund Entscheidungen für ihre Besitzer treffen. Marc Weiser beschreibt die Problematik in seinem Leitartikel zum Ubiquitous Computing wie folgt (1991): „*The [social] problem [associated with UC], while often couched in terms of pNivacy, is really one of control.*“

Wenn Objekte intelligent werden und auf Menschen automatisch reagieren, gibt es einen schmalen Grad, auf dem der Nutzensvorteil eines Dienstes gegen ein Gefühl des Kontrollverlustes bzw. realer Bevormundung abgewogen werden muss. Ein gutes Beispiel, was schon heute bekannt ist, sind Warntöne beim Nichtanschnallen im Auto: Mittels Sensoren stellt das Auto fest, dass der Fahrer nicht angeschnallt ist und zwingt die-sen daraufhin durch ein entsprechendes Warnsignal, den Schutzgurt – im eigenen Interesse! – anzulegen. Der Nutzensvorteil dieses UC-Dienstes liegt einerseits auf der Hand: die Anschnallpflicht des Fahrers wird technisch durchgesetzt und die Verletzungsgefahr desselben dadurch reduziert. Andererseits gibt es viele Menschen, die das Signal als negative Bevormundung empfinden und vielleicht sogar bewusst

einen Wagen ohne diese Funktionalität kaufen möchten.

Durch die allgegenwärtige Verfügbarkeit von Sensoren und RFID-Chips sowie entsprechender „Intelligenz“ in den Produkten besteht in Zukunft die Möglichkeit, dass ähnliche Funktionalitäten auf breiter Front entwickelt und in Produkte implementiert werden. Die Möglichkeiten der Technik können dazu genutzt werden, die Menschen darauf zu kontrollieren, ob und wie sie Regeln und Gesetze befolgen. Dies wirft insbesondere dann Probleme auf, wenn derjenige, der die Technik zu verantworten hat, unbestimmte und konkretisierungsbedürftige Rechtsregeln einseitig in seinem Sinne auslegt und über die Ausrichtung des technischen Systems, den Betroffenen „seine Auslegung“ aufzwingt. Dort, wo diese Möglichkeiten der Technik genutzt werden, um Gesetze zuzementieren, wird es zu einem Verlust von „Grauzonen“ im Umgang mit gesetzlichen Vorschriften kommen.

Fraglich ist natürlich, welchen Erfolg Hersteller haben werden, die vergleichbare Funktionen in ihre Produkte einbauen. Sicherlich gibt es für Produkthersteller ökonomische Anreize, den Gebrauch von und Umgang mit den von ihnen vertriebenen Gütern stärker zu kontrollieren. Ein Beispiel ist die Koppelung von Produkten an ihre Accessoires, wie etwa eine Bohrmaschine, die nur noch in Betrieb genommen werden kann, wenn der Heimwerker eine entsprechende Schutzbrille von demselben Hersteller trägt[4], der CD-Spieler, der CDs nur noch abspielt, wenn diese ordentlich erworben wurden (bzw. über einen entsprechenden Lizenzcode verfügen), ein Auto, das nur noch anspringt, wenn der Fahrer nachweisen kann, dass er nicht getrunken hat[5], etc. In all diesen bereits existierenden Anwendungen wird dem Menschen die Kontrolle über seine Produkte entzogen, ein „Technologiepaternalismus“ (Spiekermann und Pallas, 2005) könnte sich breit machen, der aus liberaler Sicht gesellschaftlich sicherlich nicht wünschenswert ist, aus ökonomischer Sicht jedoch sicherlich einigen Charme hat.

[1] <http://www.computerwoche.de/subnet/t-systems/857815/> (30.07.2008).

[2] [www.taucis.hu-berlin.de](http://www.taucis.hu-berlin.de).

[3] <http://www.heise.de/newsticker/Bundestag-fuer-mehr-Schutz-der-Verbraucher-vor-Telefonwerbung-/meldung/118827>.

[4] „Elektrisierende Idee“, Technology Review – Das M.I.T Magazin für Innovation, Nr. 5, 2005, S. 30.

[5] Saab: Saab unveils Alcohol Lock-Out Concept to discourage drinking and driving, Saab South Africa, 2005. Online: <http://www.saab.com/main/ZA/enlalcokey.shtml> (27.04.2005).

## Literatur

Adams, A. (2000): Multimedia information changes the whole privacy ballgame, Computers, Freedom and Privacy CFP, San Francisco, USA.

Altman, L.(1975): The environment and social behavior: Privacy, personal space, territory, crowding, Monterey, California, Brooks/Cole.

Bohn, J. / Coroama, V. et al. (2004): Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications, Journal of Human and Ecological Risk Assessment 10(5).

Boyle, M. (2003): A Shared Vocabulary for Privacy, Fifth International Conference on Ubiquitous Computing, Seattle, Washington.

Cas, J(2005): Privacy in Pervasive Computing Environments - A Contradiction in Terms?, IEEE Technology and Society 24(1), S. 24-33.

Parasuraman, A (2000): Technology Readiness Index (TRI) - A Multiple-Item Scale to Measure Readiness to Embrace New Technologies, Journal of Service Research 2(4), S. 307-320.

Spiekermann, S. / Pallas, F. (2005): Technology Paternalism - Wider Implications of RFID and Sensor Networks, Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment 4

Weiser, M. (1991): The Computer for the 21st Century, Scientific American, Issue 265, S. 94-104.

---

<https://www.humanistische-union.de/publikationen/vorgaenge/184-vorgaenge/publikation/das-internet-der-dinge/>

Abgerufen am: 19.03.2025