RWTH AACHEN UNIVERSITY

DIPLOMARBEIT

ENTWICKLUNG EINES ANWENDUNGSSZENARIOS FÜR DAS INTERNET OF THINGS IM BEREICH DER PRIVATEN BEOBACHTUNG

VON PATRICK HEINKER

LEHR- UND FORSCHUNGSGEBIET WIRTSCHAFTSINFORMATIK
PROF. DR. RER. OEC. KAI REIMERS

DIPLOMARBEIT

Zur Erlangung des Grades Diplom-Kaufmann

Entwicklung eines Anwendungsszenarios für das Internet of Things im Bereich der privaten Beobachtung

vorgelegt an der
Rheinisch-Westfälischen Technischen Hochschule Aachen
Lehr- und Forschungsgebiet Wirtschaftsinformatik

Betreuer:	Prof. Dr. rer. oec. Kai Reimers
Beratungsassistent:	Dipl.-Kfm. Thomas Wagner

von:	Patrick Heinker Bismarckstraße 106 52066 Aachen
Matr.-Nr.:	235436

Abgabetermin:	28.05.2009

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
BDSG	Bundesdatenschutzgesetz
BverfGE	Bundesverfassungsgericht
EAN	International Article Number (früher European Article Number)
EPC	Elektronischer Produktcode
etc.	und so weiter (von lat. et cetera, „und die Übrigen“)
GSM	Global System for Mobile Communications
Nr.	Nummer
RFID	Radio Frequency Identification
Tab.	Tabelle
TKG	Telekommunikationsgesetz
UHF	Ultra-High-Frequency
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network
z. B.	zum Beispiel

1 Einleitung

> *„Das Internet verbindet heute fast alle Computer der Welt, und nun macht es sich daran, auch die übrigen Gegenstände zu vernetzen.“*[1]

Die RFID-Technologie (Radio Frequency Identification) ermöglicht die eindeutige, automatisierte und vor allem kontaktlose Erfassung von Objekten, teilweise aus einer Distanz von über einem Kilometer. RFID verbreitet sich gegenwärtig rasant in immer mehr Anwendungsgebieten, besonders in der Automatisierung von Produktionsabläufen und in Lieferketten. Fallende Preise der Systemkomponenten führen dazu, dass diese Technologie immer stärkeren Einzug in unseren Alltag erhält. Bekannte Anwendungen sind hier beispielsweise elektronische Skipässe, Mautsysteme, die elektronische Wegfahrsperre oder auch der neue elektronische Reisepass. Geht es nach den Vorstellungen zahlreicher Befürworter dieser Technologie, sollen künftig sämtliche Alltagsgegenstände mit kleinen Mikrochips versehen werden, um eine weltweit eindeutige elektronische Identifikation von Objekten zu ermöglichen. In Kombination mit dem heutigen Internet könnte so mittelfristig ein „Internet der Dinge“ entstehen, welches gänzlich neue Anwendungen, aber auch Gefahren hervorbringen würde.

Die Tatsache, dass Mikrochips nahezu unsichtbar an Gegenständen angebracht und ohne Sichtkontakt – auch heimlich – ausgelesen werden können, sorgt für starke Bedenken bei Datenschützern und Verbraucherschutzorganisationen. So könnten Person- und Bewegungsprofile erstellt und ausgewertet werden, welche auf unsere Vorlieben, unsere Laster und auch auf unsere sozialen Kontakte schließen ließen. Es ist daher kaum verwunderlich, dass im Zusammenhang mit der RFID-Technologie auch stets das Risiko der totalen Überwachung durch Staat, Unternehmen, neugierige Nachbarn oder auch durch Kriminelle thematisiert wird, welches unserem Grundrecht auf informelle Selbstbestimmung entgegensteht. Gegenstand dieser Arbeit ist daher die zentrale Frage, wie stark der Einsatz der RFID-Technologie künftig zu Beobachtung, Verknüpfung und Auswertung von Konsumentenverhalten sowie der Ausnutzung von privaten Daten führen kann. Am Beispiel von zwei realistischen Zukunftsszenarien, welche im Rahmen dieser Arbeit entwickelt werden, sollen zukünftige Anwendungen der RFID-Technologie im Jahre 2020 illustriert und

---

[1] MATTERN, F. (2003), S. 1

anschließend auf ihre Gefahr bezüglich der privaten Beobachtung hin analysiert werden. Dazu wird sowohl auf die aktuelle nationale als auch auf die europäische Rechtsprechung zurückgegriffen.

Die vorliegende Arbeit untergliedert sich in sieben Kapitel, welche aufeinander aufbauen. Nachdem die Problemstellung bereits gerade einleitend dargestellt worden ist, werden in Kapitel 2 allgemeine Grundlagen zum Untersuchungsfeld aufgebaut. Hier werden zunächst die RFID-Technologie und die Vision des „Internets der Dinge“ beschrieben. Anschließend wird die essentielle gesellschaftliche Bedeutung von Privatheit erläutert und die Möglichkeiten ihrer Überwachung mittels RFID skizziert. Die damit aufgebauten Grundlagen stellen als Situationsanalyse bereits den ersten Teilschritt in der Szenarioentwicklung mittels Szenario-Technik dar. Diese Technik wird in Kapitel 3 ausführlich beschrieben, da sie im weiteren Verlauf der Arbeit als wissenschaftliche Methode angewendet wird. Die eigentliche Entwicklung zweier realistischer Zukunftsszenarien erfolgt in Kapitel 4. Hier werden zuerst relevante Einflussbereiche auf die zukünftige Entwicklung des Untersuchungsfeldes identifiziert. Aus diesen Bereichen werden einzelne Einflussfaktoren zu sogenannten „Deskriptoren“ zusammengefasst. Nachdem diese in ihrem gegenwärtigen Zustand beschrieben worden sind, werden auf Grundlage von Hintergrundrecherche jeweils zwei mögliche Zukunftsprojektionen beschrieben, die sowohl eine positive als auch eine negative Entwicklungsrichtung berücksichtigen. Die damit beschriebenen Zukunftsszenarien werden in Kapitel 5 zusammenfassend illustriert. Zwei Geschichten aus dem Leben eines Menschen beschreiben hier, wie stark technologische Anwendungen Einfluss auf unseren Alltag nehmen könnten und welche Überwachungspotenziale dadurch entstehen würden. Ob diese beschriebenen Überwachungspotenziale im Rahmen der deutschen und europäischen Rechtsprechung realisierbar sind, wird in Kapitel 6 analysiert. Nachdem die zur Bewertung relevanten Gesetze identifiziert und kurz in ihren Grundlagen sowie Anwendungsbereichen beschrieben worden sind, folgt die rechtliche Beurteilung der beschriebenen Anwendungen. Es wird überprüft, ob im Rahmen der aktuellen Rechtsprechung die Gefahr einer Überwachung durch RFID besteht, und es werden mögliche Grenzen der Rechtsprechung aufgezeigt. Im Anschluss wird eine mögliche Modernisierung des Bundesdatenschutzgesetzes vorgestellt. Die Arbeit endet in Kapitel 7 mit einer Zusammenfassung der Ergebnisse.

2 Thematische Grundlagen und Eingrenzungen des Untersuchungsfeldes

Wie funktioniert die RFID-Technologie, und in welchen Anwendungsbereichen kann sie eingesetzt werden? Wie könnte sich die Technologie weiterentwickeln, und was hat das Internet der Dinge damit zu tun? Welche Gefahren der Überwachung können durch RFID entstehen, und warum ist unsere Privatsphäre so schützenswert? Das vorliegende Kapitel beschäftigt sich mit diesen Fragen und versucht, dem Leser zunächst einige thematische Grundlagen zu vermitteln, bevor im weiteren Verlauf der Arbeit mögliche zukünftige Anwendungsszenarien entwickelt und bewertet werden. Ziel dieses Kapitels ist die Beschreibung der gegenwärtigen technischen und sozialen Situation des Untersuchungsfeldes sowie einer abschließenden Eingrenzung im Hinblick auf die weitere Szenarioentwicklung.

2.1 Technische Grundlagen

RFID gilt heute als wichtige Basistechnologie für das Internet der Dinge. Zukünftige Weiterentwicklungen dieser Technologie sollen Objekten auch eine eigene „Wahrnehmung" ihrer Umwelt ermöglichen, und damit eine allgegenwärtige Datenverarbeitung (engl. Ubiquitous Computing) ermöglichen. Nachfolgend werden die Konzepte des „Internet der Dinge" und des „Ubiquitous Computing" näher beschrieben. Es folgt eine kurze Darstellung der RFID-Technologie und ihrer heutigen Anwendungsgebiete.

2.1.1 Das Internet der Dinge und Ubiquitous Computing

Versucht man, in der Literatur eine Definition des Begriffes „Internet der Dinge" zu finden, wird man zunächst mit Begriffen wie „Ambient Intelligence" (Umgebungsintelligenz), „Pervasive Computing" (durchdringende Informationsverarbeitung) und „Ubiquitous Computing" konfrontiert. Unter diesen Begriffen fasst MATTERN[2] die Vision von intelligenten Umgebungen und smarten Alltagsgegenständen zusammen, welche, mit digitaler Logik, Sensorik und der Möglichkeit zur drahtlosen Vernetzung ausgestattet, ein „Internet der Dinge" bilden, in dem der Computer als eigenständiges Gerät verschwindet und in den Objekten der physischen Welt aufgeht. MARC WEISER gilt als Vordenker dieser Idee und führte bereits im Jahre 1991 in seinem visionären Aufsatz „The Computer for the 21st Century"[3] erstmals den Begriff „Ubiquitous Computing" ein. Er beschrieb, wie der Computer als Gerät durch „intelligente Gegenstände" ersetzt wird, welche Menschen bei ihren Tätigkeiten unauffällig und allgegenwärtig unterstützen.

---

[2] MATTERN, F. (2007), S. 11

[3] WEISER, M. (1991), S. 1

Das Internet der Dinge ist nach Definition des Bundesministeriums für Wirtschaft und Technologie (BMWi) die technische Vision, Objekte jeder Art in ein universales digitales Netz zu integrieren. In seiner einfachsten Form könne das Internet der Dinge Objekte identifizieren, aber nichts aktiv mit ihnen „tun"; in seiner komplexesten Form ließe es Objekte miteinander kommunizieren, so dass das Internet der Dinge und das Ubiquitous Computing einander ergänzen.[4]

In Visionen von möglichen Anwendungen des Ubiquitous Computing beschreibt MATTERN[5] intelligente Dinge, die wissen, wo sie sich gerade befinden, welche anderen Gegenstände oder Personen in ihrer Nähe sind und was in der Vergangenheit mit ihnen geschah. Unter dem Begriff „wearable computing" (tragbare Informationstechnologie) beschreibt er miniaturisierte Informationstechnologien, welche in Form von Kleidung, Uhren oder Schmuck in naher Zukunft unsere Umwelt wie mit unseren Augen erfassen und unsere ständigen Begleiter werden. Sensornetze würden die Eigenschaften unserer Umgebung (beispielsweise Temperatur, Luftfeuchtigkeit, Strahlung) an Millionen Stellen aufnehmen und uns damit vollkommen neue Erforschungsmöglichkeiten unserer Umwelt ermöglichen.

Bevor jedoch intelligente Gegenstände durch allgegenwärtige und alles durchdringende Informationstechnologien Einzug in unseren Alltag erhalten, sind nach Ansicht von FERSCHA[6] drei technologische Entwicklungsstufen zu durchlaufen. In der ersten Stufe stehe dabei die Vernetzung von Dingen – welche bereits beispielsweise durch die RFID-Technologie und dem heutigen Internet weit fortgeschritten sei. Es folge das „Einander-bewusst-Machen" von Menschen und Dingen sowie Dingen und Dingen, beispielsweise durch Sensoren und Kommunikationstechnologien, und letztlich folge das unsichtbare und intelligente Handeln der Objekte oder ihrer Umgebungen.

Produktinformationen mit Hilfe des Internets jederzeit verfügbar zu machen, ist die Grundidee von EPC-Global[7], einer weltweiten Non-Profit-Organisation, welche sich heute maßgeblich für die Entwicklung und Standardisierung des Internets der Dinge bemüht. Aufbauend auf dem Fundament des heutigen Internets, dem Domain Name Service (DNS), soll ein weiterer Dienst nun auch die Schnittstelle zu den Dingen herstellen: der Object Name Service (ONS). Der ONS stellt dabei ein zentrales Verzeichnis von Herstellern dar, das

---

[4] BMWI (2007B), S. 9

[5] MATTERN, F. (2008), S. 3

[6] FERSCHA, A. (2007), S. 3

[7] GS1 (2005), S. 3-5

Abfragen von Produktinformationen steuern soll und über das Produkte eine eindeutige Repräsentation im Internet bekommen sollen.

Für MATTERN steht fest, dass das Internet der Dinge als Systemelement des Ubiquitous Computing nachhaltige Auswirkungen auf viele Wirtschaftsprozesse und Lebensbereiche haben wird[8]. Die Europäische Kommission sieht große Produktivitäts- und Effizienzverbesserungen sowie neue Dienstleistungen auf unsere Gesellschaft zukommen.[9] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht sogar eine neue technologische Revolution vorher.[10]

Das Internet der Dinge und Ubiquitous Computing sind noch Zukunft. Doch die RFID-Technologie als zentraler Schritt zur weiteren integrierten Technikentwicklung[11] ist bereits heute weit entwickelt und verbreitet sich rasant in immer mehr Anwendungsbereichen. Sie sei daher im Folgenden näher beschrieben.

2.1.2 Die RFID-Technologie

2.1.2.1 Technologie

Die eindeutige, automatische und drahtlose Identifikation von Objekten ist eine der wichtigsten Voraussetzungen für die Realisierung des Internets der Dinge und von Ubiquitous Computing. Eine für diesen Zweck besonders gut geeignete Technologie ist RFID. Ein RFID-System (radio frequency identification) ist ein automatisches Identifikationssystem, mit dessen Hilfe Objekte oder Personen eindeutig gekennzeichnet und identifiziert werden können. Die Datenübertragung erfolgt durch magnetische oder elektromagnetische Felder.[12] Andere bekannte automatische Identifikationssysteme sind beispielsweise der Barcode oder die Chipkarte auf Bank- und Kundenkarten.

Die zugrunde liegenden physikalischen Prinzipien wurden zum ersten Mal Ende des zweiten Weltkrieges zur Freund-Feind-Identifikation eingesetzt.[13] Im Jahre 1948 wurde die heute bekannte RFID-Technologie durch Harry Stockman[14] erfunden. In den 60er Jahren wurde die

---

[8] MATTERN, F. (2008), S. 3

[9] EC (2008), S. 3

[10] BSI (2004), S. 12

[11] BSI (2004), S. 12

[12] FLUSSMANN, N. (2001), S. 829

[13] WIKIPEDIA.DE (2009)

[14] LANDT, J. (2001), S.4

Technologie erstmals durch Ein-Bit-Transponder im Bereich der Produktsicherung angewendet. In den 70er und 80er Jahren wurde die Technologie weiterentwickelt und gelangte in der Tierkennzeichnung und in Zugangskontrollsystemen zur Anwendung. Seitdem wurden immer mehr Anwendungsbereiche erschlossen. Die gestiegene Nachfrage hat seit 2000 für fallende Preise bei den Systemkomponenten gesorgt. Durch die parallele Entwicklung leistungsfähiger Computer und durch die Entwicklung des heutigen Internets wurden zahlreiche neue Anwendungsbereiche für RFID möglich. Heute ist RFID dabei, den Massenmarkt zu erobern.

Üblicherweise besteht ein RFID-System aus zwei Komponenten:[15] Einem Transponder (auch „Tag“ oder „Chip“ genannt) und einem Lesegerät. In der Literatur wird teilweise auch die verarbeitende Computerapplikation als dritte Systemkomponente angesehen.[16] Abbildung 1 verdeutlicht den Zusammenhang der Komponenten.

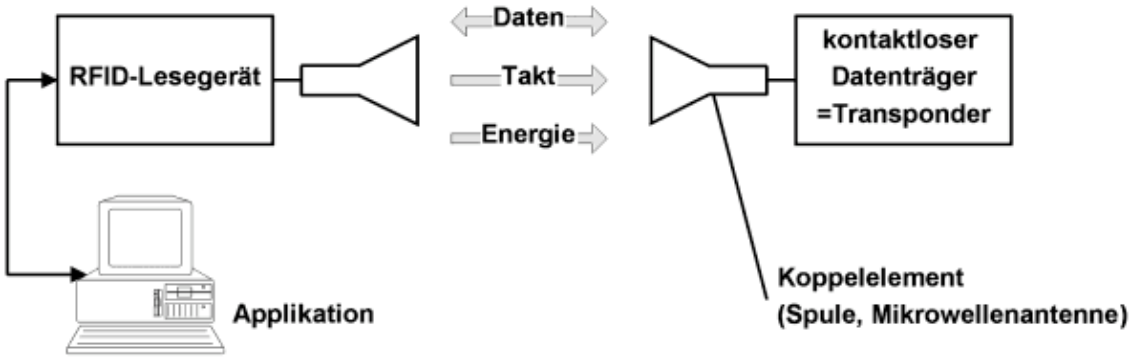

Abb. 1: Bestandteile eines RFID-Systems nach FINKENZELLER[17]

Der Transponder wird an dem zu identifizierenden Objekt angebracht. Er besteht aus einem Mikrochip und einem Koppelelement, welches als Antenne dient. Der Mikrochip beinhaltet üblicherweise eine eindeutige Identifikationsnummer und gegebenenfalls weitere Daten. Die Speicherkapazität liegt heute je nach System zwischen 1 Bit und 100 Kilobyte.[18] In der Regel besitzt der Transponder keine eigene Energieversorgung und verhält sich vollkommen passiv. Erst innerhalb des Ansprechbereiches eines Lesegerätes wird der Transponder aktiviert. Die

[15] FINKENZELLER, K. (2002), S. 7

[16] STRASSNER, M., FLEISCH, E. (2005), S. 45-54

[17] FINKENZELLER, K. (2002), S. 7

[18] FINKENZELLER, K. (2002), S. 24

zum Betrieb des Transponders benötigte Energie wird ebenso wie Takt und Daten durch die Koppeleinheit zum Transponder übertragen.
Das Lesegerät, welches aus einem Hochfrequenzmodul, einem Controller und einer Antenne besteht, erkennt den Transponder und kommuniziert mit diesem unter der Voraussetzung, dass sich der Transponder in einer angemessenen Reichweite befindet. Die Reichweite definiert sich durch die physikalischen Parameter des Systems, auf die später nochmals eingegangen wird. Das Lesegerät dient dazu, die Identifikationsnummer und – falls vorhanden – die weiteren Daten aus dem Chip auszulesen. Bei wiederbeschreibbaren Transpondern kann das Lesegerät auch Daten auf den Transponder schreiben. Die Transponderdaten des Lesegerätes können auf einen Computer übertragen werden. Dort können diese mit Datenbanken abgeglichen, verknüpft und weiterverarbeitet werden.
Transponder sind in vielen Bauformen und Ausführungen erhältlich. Grundsätzlich werden aktive und passive Transponder unterschieden. Die meisten Transponder sind passive Transponder (auch „Smart Tags“ genannt) und besitzen keine eigene Energieversorgung. Sie haben eine geringe Reichweite (wenige Zentimeter) und benötigen leistungsstarke Lesegeräte. Dafür sind sie mit einem momentanen Stückpreis von 10-30 Cent[19] relativ günstig. Aktive Transponder (teilweise auch „Semi-passive Transponder“ genannt) besitzen eine eigene Energiequelle. Normalerweise befinden sie sich im Ruhezustand bzw. senden keine Informationen aus um die Lebensdauer der Energiequelle zu erhöhen. Sie haben eine hohe Reichweite von bis zu 1 Kilometer.
Am meisten verbreitet sind heute Transponder mit einem WORM-Speicher (write-once-read-many-times). Dieser wird einmalig mit der Identifikationsnummer des Chips beschrieben und kann beliebig oft ausgelesen werden. Andere Transponder können auch einen zusätzlichen Datenspeicher oder sogar komplexe Speicherstrukturen mit Sicherheitsmerkmalen besitzen. Diese Mikrochips können beschrieben und gelesen werden.
Transponder sind, abgestimmt auf ihren jeweiligen Anwendungsbereich, in verschiedenen Bauformen erhältlich:[20]

1.) *Smart Labels* eignen sich für Preisauszeichnungen und im Logistikbereich. Der Transponder ist hier auf einem Identifikationsetikett aus Papier oder Kunststofffolie angebracht.

---

[19] INFORMATIONSFORUM RFID (2008), S. 9

[20] FINKENZELLER, K. (2002), S. 14-22 sowie BSI (2004), S. 28

2.) *Glaszylinder-Transponder* eignen sich aufgrund ihrer sehr kleinen Abmessung für die Tieridentifikation und für Wegfahrsperren.
3.) *Transponder in Kunststoffhülle* für Anwendungen mit Feuchtigkeitseinwirkungen.
4.) *Metallische Industrietransponder* für Anwendungen im Bereich der industriellen Fertigung mit besonderen Anforderungen an Hitze- und Chemikalienbeständigkeit.
5.) *Großformatige Transponder* mit hoher Reichweite für Anwendungen in der Container- und Waggonlogistik.
6.) *Card-Transponder* im Scheckkartenformat als Zugangskontrolle, für Ticketing oder Kunden- und Bonuskarten.

RFID-Systeme können unterschiedliche Frequenzen nutzen. Der Frequenzbereich hat dabei Auswirkungen auf die Sendeeigenschaften und somit auf die Einsatzgebiete des Systems.

Parameter	**Niedrigfrequenz**	**Hochfrequenz**	**Ultrahochfrequenz**	**Mikrowelle**
Frequenz	125 – 134 kHz	13,56 MHz	868 bzw. 915 MHz	2,45 bzw. 5,8 GHz
Leseabstand	bis 1,2 m	bis 1,2 m	bis 4 m	bis zu 15 m (in Einzelfällen bis zu 1 km)
Lesegeschwindigkeit	langsam	je nach ISO Standard	schnell	sehr schnell (aktive Transponder)
Feuchtigkeit	kein Einfluss	kein Einfluss	negativer Einfluss	negativer Einfluss
Metall	negativer Einfluss	negativer Einfluss	kein Einfluss	kein Einfluss
Ausrichtung des Transponders beim Auslesen	nicht nötig	nicht nötig	teilweise nötig	immer nötig
Weltweite Frequenz	ja	ja	teilweise (EU/USA)	teilweise (nicht EU)
Heutige ISO-Standards	11784/85 und 14223	14443, 15693 und 18000	14443, 15693 und 18000	18000
Typische Transponder-Bautypen	Glasröhrchen-Transponder, Transponder im Plastikgehäuse, Chipkarten Smart Label, Chipkarten	Smart Label, Industrie-Transponder	Smart Label, Industrie-Transponder	Großformatige Transponder
Beispielhafte Anwendungen	Zutritts- und Routenkontrolle, Wegfahrsperren, Wäschereinigung, Gasablesung	Wäschereinigung, Asset Management, Ticketing, Tracking & Tracing, Pulk-Erfassung	Palettenerfassung, Container-Tracking	Straßenmaut, Container-Tracking

Tab. 1: Kenngrößen von RFID-Technologien in Anlehnung an BSI (2004)[21]

Tabelle 1 vermittelt einen Überblick der weltweiten Frequenzbereiche von RFID-Systemen und deren Eigenschaften. Niedrigfrequenz-Systeme (125-134 kHz) haben eine sehr geringe

[21] BSI (2004), S. 29

Reichweite, können aber einige Materialien besser durchdringen.[22] Die Herstellungskosten für Transponder sind im niedrigen Frequenzbereich am geringsten. Je höher die Frequenzen werden, desto höher sind auch Reichweite und Lesegeschwindigkeit. Im Handel wird heute bevorzugt der Hoch- und Ultrahochfrequenzbereich genutzt, da hier auch mit passiven Transpondern eine schnelle Erfassung aus einer Reichweite von bis zu 4 Metern möglich ist. In der Literatur werden RFID-Systeme nach ihrer Leistungsfähigkeit in LowEnd-, mittlere Leistungsfähigkeit und HighEnd-Systeme klassifiziert. Für eine detaillierte Beschreibung dieser Gruppen sei an dieser Stelle jedoch auf weiterführende Literatur verwiesen.[23] Der länder- und unternehmensübergreifende Einsatz der RFID-Technologie ist nur durch die Entwicklung und Anwendung von einheitlichen Standards möglich. Derzeit lassen sich hier zwei Entwicklungsrichtungen verfolgen:[24] die International Organization for Standardization (ISO) vereinigt über 150 nationale Standardisierungsorganisationen, darunter auch das Deutsche Institut für Normung (DIN). Sie bringt einen Großteil der relevanten RFID-Standards heraus, darunter beispielsweise ISO 14443 und ISO 15693, welche für den Austausch zwischen Transponder und Lesegerät weltweit anerkannt sind. Zur Zeit sind jedoch noch anwendungsnahe Aspekte, wie etwa Datenformate und Inhalte, offen.

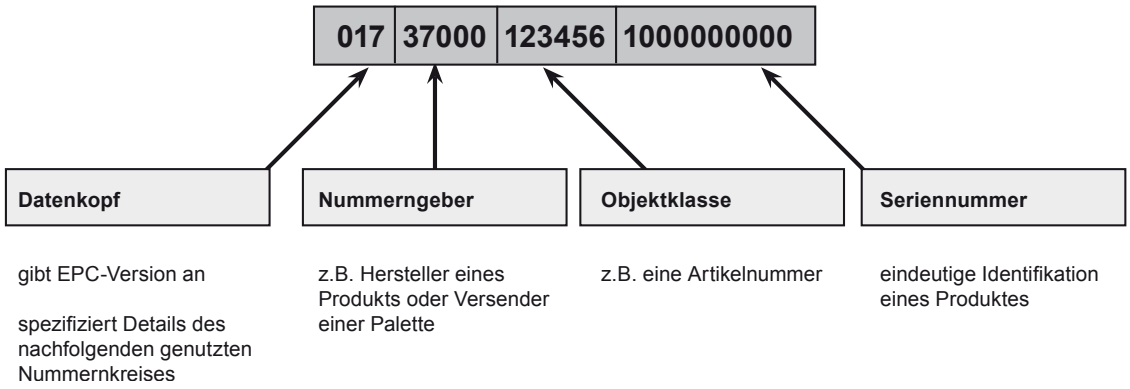

Abb. 2: Der elektronische Produktcode (EPC) von GS1[25]

Die andere Entwicklungsrichtung geht vom globalen Konsortium GS1 aus, welches sich für die wirtschaftlichen und technischen Standards des EPC-Netzwerkes einsetzt. Das EPC-Netzwerk ist eine spezielle Systemarchitektur, mit deren Hilfe Anwender auf den

---

[22] FINKENZELLER, K. (2002), S. 13

[23] z.B. BSI (2004), S. 38-39

[24] RFID-READY.DE (2009) und BMWI (2007), S. 15-19

[25] BMWI (2007A), S. 29 und GS1 (2005), S.6

elektronischen Produktcode (EPC) zugreifen können. Der EPC ist ein Nummerncode, der auf dem RFID-Chip gespeichert ist und Produkte weltweit eindeutig kennzeichnet.

2.1.2.2 Einsatzgebiete

Die Einsatzmöglichkeiten für RFID-Systeme sind vielfältig. Sie eignen sich grundsätzlich für alle Bereiche, in denen die automatische Kennzeichnung, Erkennung, Registrierung, Lagerung und Überwachung oder der automatische Transport von Objekten erforderlich sind. Auf folgenden Gebieten findet die RFID-Technologie derzeit bereits in einigem Umfang Anwendung:[26]

1.) *Logistik / Lagermanagement / Transport:* Steuerung, Überwachung und Optimierung von Liefer- und Lagerungsprozessen, beispielsweise bei Postdienstleistungen und Flughäfen
2.) *Prozesskontrolle / Produktion:* automatisierte Arbeitsprozesse, beispielsweise in der Automobilindustrie
3.) *Zahlungssysteme / Zugangskontrolle:* beispielsweise Skipässe, Mitgliedsausweise, Eintritts-, Kunden-, Schlüssel- und Signaturkarten, Geräte zur Fernablesung des Wärmeverbrauchs nach der Heizkostenverordnung
4.) Wegfahrsperren: Der Tag befindet sich bei dieser Applikation im Autoschlüssel, das Lesegerät im Zündschloss
5.) *Landwirtschaft / Qualitätskontrolle*: Erfassung und Kennzeichnung von Tierbeständen, lückenlose Herkunftskontrolle von Fleischwaren
6.) *Arbeitswelt*: Zeiterfassung, Zugangskontrolle und Authentifizierung

In den folgenden Bereichen befindet sich die RFID-Technologie zurzeit in der Erprobung:

1.) *Endkundenbereich*: Bezahlvorgänge, Produktinformationsterminals
2.) ÖPNV: Automatisierte Abrechnungssysteme
3.) Archivierungssysteme: Bestandserfassung, Diebstahlschutz und Optimierung von Ausleihvorgängen in Bibliotheken
4.) Identitäts- und Echtheitsnachweis / Bekämpfung von Diebstahl und Produktpiraterie: ePass, auf Veranstaltungstickets sowie auf Arzneimitteln und Luxusartikeln
5.) Sport: Nachverfolgung von Streckenabschnitten

---

[26]BMI (2008), S. 4-6

6.) *Gesundheitssystem:* Vermeidung von Patientenverwechslungen, Verfolgung von Infektionswegen, Optimierung der Auslastung von medizinischen Geräten, Bestandsverwaltung

Eine im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi) erstellte Studie kommt zu dem Ergebnis, dass im Jahr 2010 ca. 8 Prozent der Bruttowertschöpfung in wichtigen Bereichen des produzierenden Gewerbes, des Handels, des Verkehrs sowie der privaten und öffentlichen Dienstleister von RFID beeinflusst sein werden. In den letzten fünf Jahren hat sich der Einsatz von RFID in Deutschland hier bereits verzehnfacht.[27] Dies ist nach Auffassung des BMWi ein deutliches Indiz dafür, dass RFID schon mittelfristig eine bedeutende Rolle als Querschnittstechnologie einnehmen wird.

2.2 Informelle Privatheit und Möglichkeiten ihrer Überwachung

Die Beschreibung der technischen Möglichkeiten des Internets der Dinge und der RFID-Technologie lassen bereits erahnen, dass gänzlich neue Möglichkeiten in der Überwachung von Menschen entstehen können, wenn künftig immer mehr Produkte des alltäglichen Lebens mit RFID- Transpondern versehen werden. Befürchtungen der totalen Überwachung unserer Privatheit sind bereits seit mehreren Jahren Gegenstand zahlreicher Veröffentlichungen und stehen gegenwärtig im Mittelpunkt der öffentlichen Wahrnehmung, wenn es um diese Zukunftstechnologien geht. Doch was zeichnet Privatheit aus, und warum ist sie von grundlegender Bedeutung für unsere Gesellschaft? Welche Grenzbereiche bestimmen unsere Privatheit, und wie stark sind diese durch neue technologische Entwicklungen im Bereich von RFID bedroht? Im folgenden Abschnitt sollen diese Fragen beantwortet werden.

2.2.1 Informelle Privatheit

Um die Bedeutung der informellen Privatheit, im Folgenden auch Privatsphäre genannt, zu verstehen, ist zunächst eine Auseinandersetzung mit dem Begriff „Privatheit“ notwendig. Das deutsche Wort „privat“ wird seit dem 16. Jahrhundert verwendet und bezeichnet Sachverhalte beziehungsweise Personen, die für sich stehen, also unabhängig sind.[28]

---

[27] BMWI (2007A), S. 4

[28] SCHAAR, P. (2007), S. 16

LANGHEINRICH beschreibt Privatheit unter Bezug auf eine Definition von RÖSSLER[29] als die Autonomie des Individuums, also der Fähigkeit, die Frage nach der Person, die man sein will, zu stellen und zu beantworten und dann – im Privaten – auch tatsächlich nach den eigenen Wünschen zu leben. In ähnlicher Form, allerdings etwas stärker zugeschnitten auf die moderne Informationsverarbeitung, zitiert LANGHEINRICH die informelle Privatheit in einer Definition von WESTIN[30] wie folgt:

> *„Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others."*

Die grundlegende Bedeutung der Privatsphäre für die Weiterentwicklung und den Erhalt unserer Demokratie beschreibt SCHAAR[31], Bundesbeauftragter für den Datenschutz, unter Verweis auf TINNEFELD[32]. So sei die Privatsphäre Raum des individuellen Rückzugs und zugleich unverzichtbare Voraussetzung einer freien Meinungsbildung. Ohne einen geschützten Raum, in dem man unbeobachtet und unzensiert über seine Erfahrungen und Einstellungen reflektiert und sich mit anderen austauscht, könne es auch keine freie Öffentlichkeit geben. Freie Rede, freie Information und freie Meinungsäußerung würden ohne ein tief verankertes Recht auf Privatheit verkümmern. Datenschutzgesetzte sollen deshalb die Würde, Privatsphäre und Handlungsfreiheit der Individuen gewährleisten. In Deutschland spiegelt sich das Streben nach dem Erhalt von Privatsphäre, welches im Rahmen des Volkszählurteils 1982 aus Art. 1 des deutschen Grundgesetzes zur Menschenwürde abgeleitet wurde, rechtlich im Begriff der „informationellen Selbstbestimmung" wider.
Soziologisch wird der Prozess, mit dem Menschen ihre Privatsphäre schützen oder aufgeben, nach SPIEKERMANN als eine Art „Grenzverwaltung" verstanden.[33] Um im Folgenden zu analysieren, in welchen Bereichen die Privatheit durch moderne Informationstechnologien bedroht sein könnte, seien die Grenzen der Privatheit zunächst noch etwas detaillierter dargestellt. BOHN ET AL.[34] beschreiben vier Grenzbereiche, deren Überschreitung eine

---

[29] LANGHEINRICH, M. (2004), S. 4 zitiert RÖSSLER, B. (2001)

[30] LANGHEINRICH, M. (2004), S. 4 zitiert WESTIN, A. (1967)

[31] SCHAAR, P. (2007), S. 15

[32] TINNEFELD, M. (2007), S. 626

[33] SPIEKERMANN, S., ROTHENSEE, M.: (2005), S. 6 zitiert ALTMAN, I. (1975)

[34] BOHN ET AL. (2003), S. 8-10

Verletzung der Privatsphäre von Individuen darstellen kann: natürliche Grenzen, soziale Grenzen, räumliche und zeitliche Grenzen sowie Grenzen flüchtiger Situationen.
Diese Grenzbereiche erscheinen unmittelbar nachvollziehbar. So ist die einfachste, essentielle Form zum Schutz der Privatsphäre die natürliche Grenze, also die räumliche Abschottung in der eigenen Wohnung, die Nutzung von Kleidung oder das Verschließen von Briefen. Unter einer sozialen Grenze verstehen wir unsere Erwartung an die Vertraulichkeit sozialer Gruppen. So ist es uns wichtig, dass bestimmte persönliche Informationen (beispielsweise über unsere Gesundheit) innerhalb eines bestimmten Personenkreises unseres Vertrauens bleiben. Die räumliche und zeitliche Grenze beschreibt unsere Erwartung, dass gewisse Teile unseres Lebens sowohl zeitlich als auch räumlich getrennt voneinander existieren können. Eine wilde Jungend sollte demnach nicht unser späteres Leben beeinflussen oder uns nachgetragen werden. Letztlich spielen auch das Vergessen und die Vergänglichkeit von Informationen eine wichtige Rolle, welche als Grenzen für flüchtige Situationen beschrieben werden. Wir hoffen, dass spontane Bemerkungen oder Handlungen, welche vielleicht unüberlegt waren, von unserem sozialen Umfeld vergessen werden. Daher fühlen wir uns in unserer Privatsphäre beeinträchtigt, wenn uns aus unserer Vergangenheit etwas nachgetragen wird, was wir mit unserer Gegenwart nicht mehr verbinden.

2.2.2 Möglichkeiten der Überwachung durch RFID

Wissenschaftler und Verbraucherschutzorganisationen sehen in der RFID-Technologie und im Internet der Dinge wesentliches Potential, alle beschriebenen Grenzbereiche der Privatheit zu überschreiten,[35] und sehen eine neue Qualität der Datenerfassung auf uns zukommen.[36] Nach LANGHEINRICH könnte die Ausdehnung der Datenerfassung und deren zeitliche Abdeckung viel größere Ausmaße annehmen. Ein bewusstes Begrenzen der Erhebung sei durch die unbemerkte Datenerfassung kaum mehr möglich. Dadurch würde sich auch die Art der Datenerhebung wesentlich von der heutigen Art unterscheiden, welche sich zumindest im Nachhinein noch rekonstruieren ließe, etwa wenn man an einem Gewinnspiel teilgenommen hat. Durch die automatische Erfassung von „Echtzeit-Daten“ ließe sich auch ein Profil unserer tatsächlichen Vorlieben erstellen (im Gegensatz zu von uns angegebenen Vorlieben), welches einen tieferen Einblick in unseren Charakter ermöglichen würde. Der Erhebungsgrund der Datenerfassung würde durch die permanente Erfassung nicht mehr einzugrenzen sein, und

[35] FRIEDEWALD, M. (2007), S. 207 sowie BOHN ET AL. (2003), S. 9

[36] LANGHEINRICH, M. (2004), S. 8

schließlich würde ein nicht mehr zu überblickendes Datennetz entstehen, welches sich durch traditionelle Zugriffskontrollen nicht mehr verwalten ließe.

Es ist kaum verwunderlich, dass in der Bevölkerung eine Bedrohung der Privatsphäre durch die neue Technologie empfunden wird. Berichterstattungen aus der Presse und dem Fernsehen weisen stets auf die weitreichenden Konsequenzen bis hin zum Überwachungsstaat hin,[37] und Kampagnen gegen die Einführung von RFID durch Verbraucherschutzorganisationen wie etwa dem Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD) und Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) haben diese Befürchtungen in der öffentlichen Wahrnehmung noch verstärkt.[38] Aber die Befürchtungen sind nicht unbegründet. In einem internen Arbeitspapier zum Thema „Internet der Dinge“ sieht auch die Europäische Union Handlungsbedarf im Bereich Datenschutz und Schutz der informellen Privatheit. Sie erarbeitet derzeitig eine Strategie zum zukünftigen Umgang mit diesem Thema. [39]

Doch welche Gefahren der Überwachung kommen tatsächlich auf uns zu? Unter Bezug auf eine vom Auto-ID-Center und der Humbold-Universität zu Berlin durchgeführte Verbraucheranalyse[40] beschreibt SPIEKERMANN[41] fünf Gefahrenbereiche für die Privatheit von Verbrauchern durch den Einsatz von RFID-Technologie:

1.) *Unbemerktes Auslesen durch Dritte:* Das Auslesen von RFID-Tags erfolgt berührungslos und ohne Sichtkontakt. Theoretisch kann jede Person, welche über ein Lesegerät verfügt, RFID Tags in Reichweite unbemerkt auslesen. Erste RFID-Lesegeräte sind bereits in Handys eingebaut worden.[42] Ist die Entfernung für das Auslesen zu groß, kann alternativ auch die Übertragung zwischen den Tags und anderen Lesegeräten abgehört werden. Die übertragene EPC-Nummer kann per Internet über einen ONS-Dienst einem Objekt eindeutig zugeordnet werden. Werden mehrere Objekte, welche gleichzeitig von einer Person mitgeführt werden, identifiziert, kann ein Profil dieser Person erstellt werden. Aufenthaltsorte von Individuen könnten auch über einen längeren Zeitraum hinweg zurückverfolgt werden.

---

[37] TAGESSCHAU.DE (2009), am 7.4.2009

[38] siehe dazu auch WWW.FOEBUD.ORG und WWW.NOCARDS.ORG

[39] EC (2008), S. 10

[40] BERTHOLD, O., GÜNTHER, O., SPIEKERMANN, S. (2005), S. 422-430

[41] SPIEKERMANN, S., ZIEKOW, H. (2006), S. 5

[42] NOKIA.DE (2009), am 7.4.2009

2.) *Verfolgbarkeit von Personen durch ihre Objekte:* Mitgeführte Tags in Schuhen oder Kleidung ermöglichen die eindeutige Identifizierung von Personen, auch ohne Kenntnis ihrer wirklichen Identität. Werden diese Tags von vielen Lesegeräten erfasst, lässt sich durch einen Abgleich der eindeutigen Identifikationsnummern der Tags ein Bewegungsprofil erstellen.

3.) *Auffinden sozialer Netzwerke:* Mittels intelligenter Datenverknüpfung können auch soziale Netzwerke identifiziert werden. Beobachtet man beispielsweise zwei Personen regelmäßig an den selben Orten und nahe beisammen kann schon von einer sozialen Beziehung dieser Personen ausgegangen werden.

4.) *Verantwortlichkeit für Objekte:* Die Zuordnung von Personen zu Objekten kann dazu verwendet werden, um Personen in die Verantwortung für den Missbrauch oder Verbleib dieser Objekte zu ziehen. Der Besitzer einer weggeworfenen Cola-Dose könnte dadurch identifiziert werden, aber auch lange verkaufte Objekte, die später in eine kriminelle Handlung involviert wurden, können so den Verdacht auf den früheren Besitzer lenken.

5.) *Bevormundung durch Technik:* RFID kann benutzt werden, um ein falsches Verhalten eines Individuums festzustellen, dieses womöglich öffentlich machen, sanktionieren oder automatisch unterbinden. Ein Mülleimer könnte bei dem versehentlichen Einwerfen einer Batterie einen Alarm auslösen, oder ein CD-Player die Wiedergabe einer kopierten CD verweigern. Durch RFID können Millionen solcher Beispiele möglich werden.

Das geheime oder öffentliche Auslesen von Daten kann auch zu einem Sicherheitsrisiko für Unternehmen werden. GARFINKEL[43] weist hier auf die Gefahr von Industriespionage oder gezielter Kundenabwerbung hin. Im Unternehmensbereich lassen sich ferner auch die Mitarbeiter, Kunden und Zulieferer durch die RFID-Technologie besser überwachen.

2.2.3 Schutzmaßnahmen und Sicherheitstechniken

Derzeit werden drei mögliche Schutzmaßnahmen zum Umgang mit personenbezogenen Daten diskutiert:[44] die Anwendung beziehungsweise Erweiterung bestehender Datenschutzgesetze, freiwillige Selbstverpflichtungen der Anwender und Datenschutzzertifikate. Auf

[43] GARFINKEL, S., JUELS, A., PAPPU R. (2005), S.37-38

[44] BMWI (2007A), S. 32

technologischer Basis könnten Datenschutz-Technologien (auch „privacy enhancing technologies“ oder kurz „PET“ genannt) die Sicherheit der Verbraucher erhöhen. Zurzeit werden nach LANGHEINRICH[45] zwei Ansätze für technische Lösungen im Bereich RFID-Datenschutz diskutiert: Anonymisierung und Pseudonymisierung. Dabei wird die auf dem Tag gespeicherte ID entweder verändert oder gelöscht, der Tag durch eine Zugriffskontrolle geschützt oder die Kommunikation mit dem Leser verschlüsselt. Bisher hat sich jedoch noch kein Verfahren durchsetzen können. Nachfolgend seien die verschiedenen technischen Schutzmaßnahmen kurz beschrieben:

Anonymisieurng mittels „Kill-Befehl“: Der aktuelle EPC-Global-Standard schreibt zwecks Deaktivierung von Tags einen Kill-Befehl vor, der nach Übermittlung eines Passwortes den Tag dauerhaft deaktiviert.[46] Diese extremste Form der Deaktivierung macht den Tag für jegliche weitere Anwendung unbrauchbar.

Pseudonymisierung mittels (variabler) Hash-Locks: Der Tag antwortet nicht mit seiner wahren ID, sondern mit einem verschlüsselten Wert (Meta-ID). Nur durch einen Schlüssel kann der wahre Wert identifiziert werden. Eine Weiterentwicklung ist der variable Hash-Lock, welcher bei jeder Abfrage einen anderen verschlüsselten Wert nach einem Zufallsprinzip ausgibt. Hierdurch soll das Verfolgen einer statischen Meta-ID vermieden werden.[47]

Distanz-basierte Zugriffskontrolle: RFID-Tags messen die Signalstärke der auslesenden Lesegeräte und geben in Abhängigkeit von der ermittelten Distanz mehr oder weniger Informationen preis. [48]

Abhörsichere Antikollisionsprotokolle: Hierbei wird die Datenübertragung vom Tag zum Lesegerät verschlüsselt, um persönliche Daten vor unerlaubtem „Mithören“ zu schützen. Das Verfahren wird bereits im deutschen Reisepass mit einem 112 Bit langen Schlüssel angewendet.

Blocker-Tag und Abschirmung:

Blocker-Tags bewirken eine Überlastung der Lesegeräte, so dass eine Identifikation des richtigen Signals nicht mehr möglich ist. Das Blocker-Tag simuliert dem Lesegerät eine so große Zahl adressierbarer RFID-Tags, die sich unmöglich alle nacheinander abfragen lassen.[49]

---

[45] LANGHEINRICH, M. (2004), S. 13

[46] EPCGLOBAL (2006), S. 20

[47] SARMA, S., WEIS S., ENGELS, D. (2002)

[48] FISHKIN, K., ROY, S. (2003)

[49] JUELS, A., RIVEST, R., SZYDLO, M. (2003)

Allerdings muss das Blocker-Tag mitgeführt werden. Eine andere Möglichkeit des Selbstschutzes ist die Abschirmung beispielsweise durch Alufolie. Im Internet werden bereits abgeschirmte Passhüllen und Einkaufstaschen verkauft.

2.3 Eingrenzung des Untersuchungsfeldes

Die in diesem Kapitel aufgebauten Grundkenntnisse zum Internet der Dinge, der RFID-Technologie, der Bedeutung der informellen Privatheit und deren Bedrohung durch RFID strukturieren den Problembereich dieser Arbeit und dienten der Vorbereitungsphase für die weitere Szenariobildung. Dennoch ist eine weitere Eingrenzung des Untersuchungsfeldes notwendig, da der Themenbereich sehr komplex ist. Für die nachfolgende Entwicklung der Zukunftsszenarien wurde das Untersuchungsfeld daher wie folgt abgegrenzt:

Thematisch stehen die Möglichkeiten der Überwachung von Verbrauchern durch die RFID-Technologie und das Internet der Dinge im Mittelpunkt. Andere Auswirkungen, wie etwa gesundheitliche oder wirtschaftliche Risiken der neuen Technologien, werden nicht betrachtet.

Bei der Überwachung steht dabei nur der private Sektor, also der Wirtschaftsbereich der privaten Haushalte, Organisationen ohne Erwerbszecke und privaten Unternehmen,[50] im Fokus. Hier liegt der Schwerpunkt besonders auf den privaten Haushalten. Eine Betrachtung der Überwachung durch den öffentlichen Sektor oder auch durch Kriminelle mit Hilfe der neuen Technologien würde den Umfang dieser Arbeit bei weitem sprengen.

Die Zukunftsprojektion soll für das Jahr 2020 erfolgen. Dieser Zeithorizont wurde gewählt, da er nicht allzu weit von der Gegenwart entfernt liegt – also noch modellierbar ist – und dennoch signifikante Veränderungen aufzeigen wird.

3 Die Szenario-Technik als wissenschaftliche Methode

Die Entwicklung eines Zukunftsszenarios kann auf Grundlage von verschiedenen Methoden erfolgen. Der wesentliche Anspruch an eine wissenschaftliche Methode liegt dabei in der Nachvollziehbarkeit der Szenarioentwicklung sowie in der Vermeidung von willkürlichen Behauptungen. Als methodische Grundlage dieser Arbeit wurde die Szenario-Technik ausgewählt. Der Ursprung dieser Methode, ihr Konzept und ihre Vorteile werden in diesem Kapitel beschrieben. Im Anschluss werden die einzelnen Stufen im Szenario-Prozess vorgestellt.

---

[50] DUDEN WIRTSCHAFT (2004)

3.1 Entstehung und Konzept der Szenario-Technik

Wie auch der Begriff „Strategie“ seinen Ursprung im Militär hat, ist auch der Begriff eines „Szenarios“ erstmalig in den 50er Jahren im Rahmen von militärstrategischen Planspielen entstanden. HERMAN KAHN führte in diesem Kontext den Begriff eines Szenarios ein und verstand darunter eine Situation unter vorgegebenen Rahmenbedingungen.[51] Seine 1967 veröffentlichte Studie *„The Year 2000. A Framework for Speculation on the next Thirty-Three Years“* gilt später als die Geburtsstunde der Szenarioplanung.[52]

Die Verknüpfung von komplexen Zusammenhängen und deren Wechselwirkungen gelang 1972 erstmals MEADOWS, MEADOWS UND ZAHN. In ihrer Veröffentlichung „*Die Grenzen des Wachstums*“ entwarfen sie im Auftrag des Club of Rome düstere Zukunftsbilder zur Lage der Menschheit auf Grundlage von negativen Entwicklungstrends. Ihr Ziel bestand darin, die Verantwortlichen aufzuschrecken, damit diese rechtzeitig Gegenmaßnahmen ergreifen würden um diese Szenarien zu vermeiden.[53]

Bis Ende der 60er Jahre arbeiteten die meisten Unternehmen mit dem Instrument der Prognose, um ihre zukünftige Entwicklung quantitativ zu berechnen. Die nicht vorhergesehene Ölkrise Anfang der 70er Jahre belegte jedoch, dass eine rein quantitative Planung nicht ausreichte, um komplexe Zukunftssituationen in der Gegenwart zu modellieren. Dies brachte insbesondere das Unternehmen Royal Dutch / Shell dazu, verstärkt qualitative Informationen in seiner strategischen Planung in Form von Szenarien zu berücksichtigen. Die Shell Gruppe gilt seitdem als Pionier in der Szenario-Entwicklung. Es folgten zunächst weitere Unternehmen aus der Ölbranche, und langsam etablierte sich die Szenario-Technik als ein anerkanntes wirtschafts- und sozialwissenschaftliches Planungsverfahren. Seitdem hat sich diese Methode immer stärker zu einem Planungsinstrument für Unternehmen etabliert und ist heute eng mit der strategischen Unternehmensplanung verknüpft.[54]

In der Literatur wird die Szenario-Technik häufig mit Hilfe des sogenannten Szenario-Trichters veranschaulicht (siehe Abbildung 3).[55]

---

[51] VON REIBNITZ, U. (1991), S. 12

[52] FINK, A., SCHLAKE, O., SIEBE, A. (2002), S.59

[53] MEADOWS, D., MEADOWS, D., ZAHN, E. (1972)

[54] VON REIBNITZ, U. (1991), S. 13

[55] VON REIBNITZ, U. (1991), S. 27

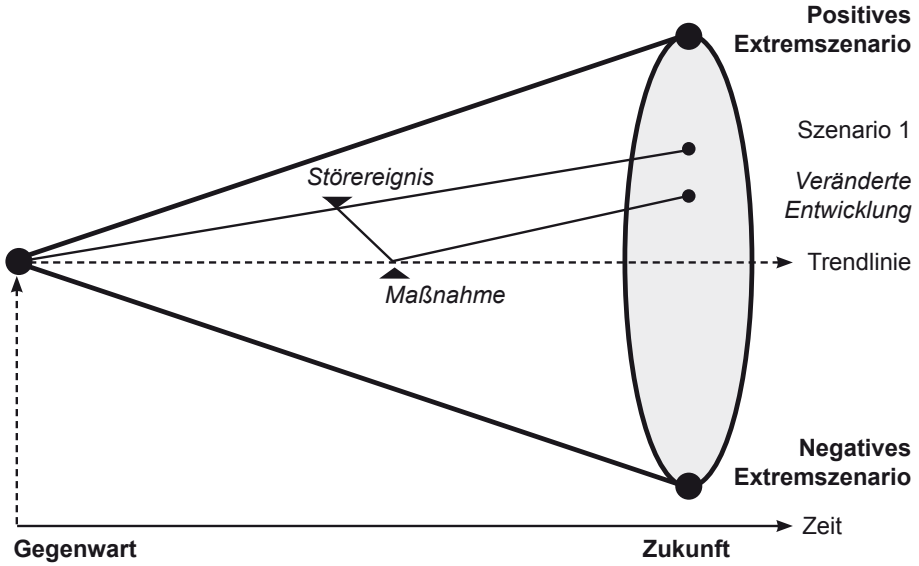

Abb. 3: Szenario-Trichter nach VON REIBNITZ

Ausgangspunkt ist dabei die Gegenwart, welche am engsten Punkt des Trichters abgebildet ist. Die Gegenwart unterliegt dem Einfluss gewisser Faktoren (zum Beispiel Märkte, Gesetze, wirtschaftliche Situation). Dieser Einfluss ist für die nahe Zukunft noch vorhersehbar. Je weiter man aber aus heutiger Situation in die Zukunft geht, desto unsicherer und komplexer wird es, diese Faktoren vorherzusehen. Störereignisse oder Gegenmaßnahmen können die Entwicklung von einzelnen Faktoren im Zeitverlauf beeinträchtigen und zu einer anderen Zukunft führen. Zieht man einen Schnitt durch den Trichter an einem beliebigen Zeitpunkt der Zukunft, dann liegen alle denkbaren Zukunftssituationen (Szenarien) auf der Schnittfläche des Trichters. Es können also unendlich viele Zukunftsszenarien entstehen.

Die Szenario-Technik entwickelt unter Berücksichtigung von quantitativen und qualitativen Informationen über die Einflussfaktoren verschiedene, stets plausible Zukunftsszenarien des Untersuchungsgegenstandes.

ABERS UND BROUX[56] sehen bei der Szenario-Technik den Vorteil darin, dass nur drei Grundtypen von Szenarien zu betrachten sind, um alle möglichen, empirisch wahrscheinlichen Szenarien beschreiben zu können: Ein positives Extremszenario, welches die günstigste Zukunftsentwicklung bezeichnet, ein negatives Extremszenario, welches den schlechtest möglichen Entscheidungsverlauf bezeichnet, sowie ein Trendszenario welches die Fortschreibung der heutigen Situation in die Zukunft beschreibt. VON REIBNITZ[57] empfiehlt

[56] ARBERS, O., BROUX, A. (1999), S.59

[57] VON REIBNITZ, U. (1991), S. 28

sogar, keine Trend-Extrapolation aus der Gegenwart in die Zukunft zu entwickeln, sondern sich auf nur zwei Szenarien zu konzentrieren, die in sich konsistent und stabil sind und sich gleichzeitig deutlich voneinander unterscheiden. Das Problem von Trend-Szenarien liege darin, dass sie lediglich die Gegenwart fortführen und somit keine neuen Erkenntnisse liefern. Eine anschauliche, zusammenfassende Definition der Szenario-Technik (auch Szenario-Methode genannt) liefert VON REIBNITZ:[58]

> *„Unter einem Szenario versteht man die Beschreibung einer zukünftigen Situation und die Entwicklung beziehungsweise Darstellung des Weges, der aus dem Heute in die Zukunft hineinführt. Unter Szenario-Methode versteht man eine Planungstechnik, die in der Regel zwei sich deutlich unterscheidende, aber in sich konsistente Szenarien (Zukunftsbilder) entwickelt und hieraus Konsequenzen für das Unternehmen, einen Bereich oder eine Einzelperson ableitet."*

Zusammenfassend liegt der Vorteil der Szenario-Technik darin, dass quantitative und qualitative Aspekte betrachtet werden. Außerdem wird die Vernetzung von Einflussfaktoren untereinander berücksichtigt, und es werden Störfaktoren beachtet. Letztlich bietet die Szenario-Technik auch die Möglichkeit, eine Strategie auf Basis von Alternativen zu entwickeln, um zukünftige Situationen zu erreichen oder zu vermeiden.

3.2 Phasen und Instrumente der Szenario-Technik

Neben einer geeigneten Definition der Szenario-Technik beschreibt VON REIBNITZ[59] auch einen idealtypischen Szenarioprozess, welcher dem Verfasser dieser Arbeit als geeignetes Vorgehen in der Entwicklung des Zukunftsszenarios erscheint. Andere Ansätze, wie etwa die Weiterentwicklung nach FINK,[60] haben ihren Schwerpunkt mehr in der strategischen Planung für Unternehmen und sind daher für ein allgemeines Szenario nur ansatzweise brauchbar. Der Prozess der Szenario-Technik gliedert sich nach VON REIBNITZ in drei Phasen und insgesamt acht Teilschritte (siehe Abbildung 4), welche nachfolgend beschrieben werden.

---

[58] VON REIBNITZ, U. (1991), S. 14

[59] VON REIBNITZ, U. (1991), S. 14

[60] FINK, A., SCHLAKE, O., SIEBE, A. (2002)

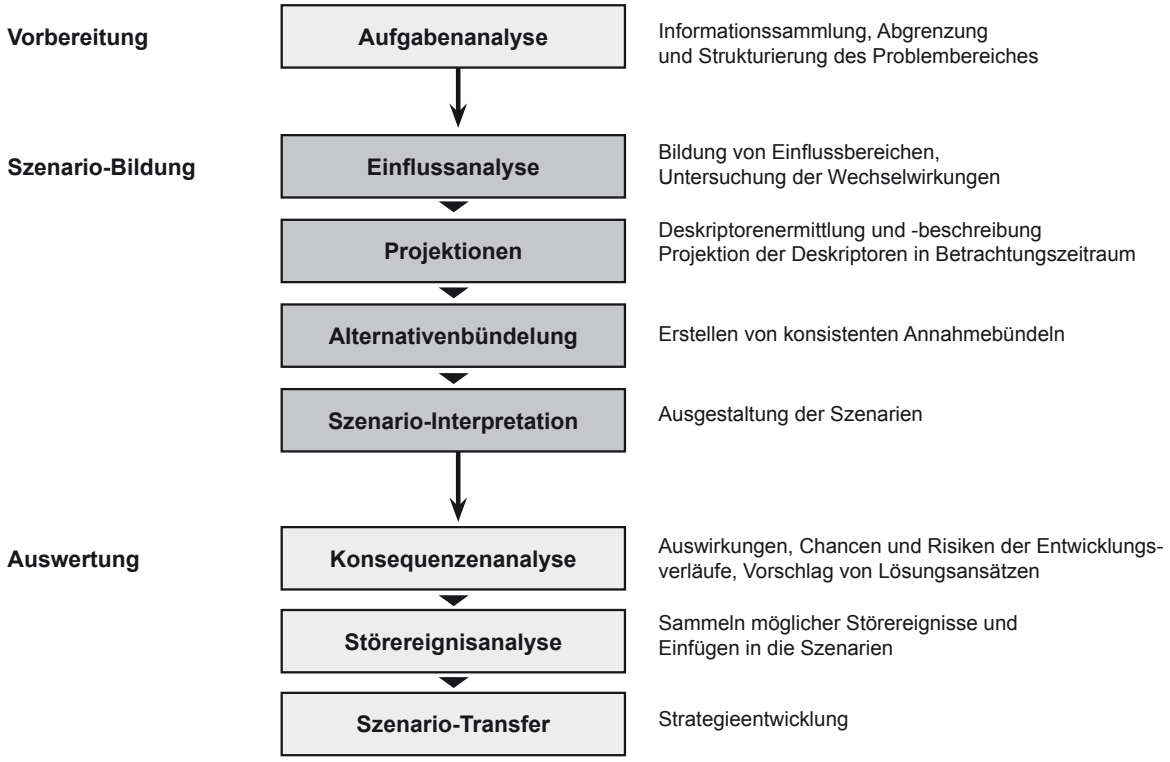

Abb. 4: Idealtypischer Szenarioprozess in Anlehnung an VON REIBNITZ[61]

Aufgabenanalyse: Die erste Phase des Szenarioprozesses ist die Vorbereitungsphase. Hier wird die momentane Situation des zu untersuchenden Gegenstandes betrachtet sowie der Betrachtungszeitraum festgelegt. Es wird dargelegt, warum der Sachverhalt untersucht wird, und welches gesellschaftliche Problem als lösungsbedürftig eingestuft wird. Für das in dieser Arbeit zu erstellende Zukunftsszenario ist die Vorbereitungsphase bereits in Kapitel 2 dieser Arbeit erfolgt. Damit sollte dem Leser ein interessanter und schneller Einstieg in die Thematik ermöglicht werden.

Einflussanalyse: Die eigentliche Szenario-Bildung erfolgt in vier Teilschritten. Zunächst werden im Rahmen einer Einflussanalyse relevante Einflussbereiche ermittelt, die auf den zu untersuchenden Gegenstand direkt oder indirekt einwirken. Typische Einflussbereiche sind etwa Politik, Ökonomie, Gesellschaft und Technologie. Innerhalb der jeweiligen Einflussbereiche werden nun relevante Einflussfaktoren ermittelt und in ihrer Bedeutung für den Untersuchungsgegenstand mit Hilfe einer relativen Rangfolge bewertet. Anschließend wird durch eine Vernetzung der Einflussbereiche analysiert, wie stark jeder Bereich alle

[61] VON REIBNITZ, U. (1991), S.30

anderen Bereiche beeinflusst. Dies führt man üblicherweise systematisch mit Hilfe einer Vernetzungsmatrix durch.[62] Diese Methode wird in Kapitel 4 angewendet.

Projektionen: Nun beginnt der „Blick in die Zukunft". Ziel dieses Schrittes ist es, auf der Basis der bereits ermittelten Einflussfaktoren beschreibende Kenngrößen (im weiteren Verlauf Deskriptoren genannt) zu ermitteln, welche den jetzigen und zukünftigen Zustand der jeweiligen Entwicklungen beschreiben. Nach VON REIBNITZ[63] sollte dabei größtmöglicher Wert auf eine wertneutrale Formulierung gelegt werden, um in der Ausarbeitung den möglichen zukünftigen Entwicklungen nicht schon tendenziöse Richtungen zu verleihen. Es sollte auch auf den Einsatz von Eintrittswahrscheinlichkeiten verzichtet werden, da diese den Blick für die möglichen alternativen Zukünfte verengen würden. Der Ausarbeitung der Deskriptoren liegt eine umfangreiche Informationsrecherche zu Grunde, in der sowohl quantitative als auch qualitative Aspekte bewertet werden. Ist der Deskriptor in seinen Ist-Zustand beschrieben, projiziert man ihn in den nächsten Zeithorizont. Die weitere Entwicklung kann dabei eindeutig oder unsicher sein. Im ersten Falle spricht man von einem eindeutigen Deskriptor. Ist die zukünftige Entwicklung unsicher, müssen alternative Entwicklungsrichtungen beschrieben und begründet werden. Hier spricht man von einem alternativen Deskriptor.

Alternativenbündelung: Die entwickelten alternativen Zukunftsprojektionen werden nun zu Projektionsbündeln zusammengestellt, welche zwei in sich konsistente und von einander deutlich unterschiedliche Rohszenarien beschreiben. Bei einer geringen Anzahl von Deskriptoren, also bei etwa 12-15, kann die Beurteilung durch einen intuitiven Prozess der Beurteilung der Konsistenz geschehen. Bei einer größeren Anzahl von Deskriptoren sollte eine Konsistenzanalyse mit Hilfe einer Konsistenzmatrix erfolgen. Der Aufbau und Ablauf einer Konsistenzanalyse mit Hilfe einer Konsistenzmatrix wird hier aber nicht näher beschrieben, da in der weiteren Szenario-Bildung eine intuitive Beurteilung der Konsistenz möglich ist.

Interpretation: Auf Basis der Rohszenarien des vorhergehenden Schrittes werden in diesem letzten Schritt der Szenario-Bildung die beiden unterschiedlichen, in sich plausiblen und konsistenten Szenarien herausgebildet und textlich beschrieben. Dies kann zum Beispiel über eine Storyline, also die Beschreibung einer zukünftigen Alltagssituation, erfolgen, worin die jeweiligen Ausprägungen der jeweiligen Deskriptoren integriert wurden.

---

[62] VON REIBNITZ, U. (1991), S. 35

[63] VON REIBNITZ, U. (1991), S. 45

Konsequenzenanalyse, Störereignisanalyse und Szenario-Transfer: Die Szenario-Technik wird, wie bereits beschrieben, häufig im Kontext der strategischen Unternehmensplanung eingesetzt. Welche Chancen und Risiken sich aus den beiden skizzierten, unterschiedlichen Zukunftsbildern ergeben können, und mit welchen Maßnahmen darauf zu reagieren ist, wird im Rahmen der Konsequenzenanalyse herausgestellt.
In der Störereignisanalyse werden unvorhersehbare, plötzliche Ereignisse gesammelt, welche sowohl positive als auch negative Auswirkungen haben können. Anschließend können entsprechende Präventiv- und Reaktivmaßnahmen beschrieben werden. In dieser Arbeit wird auf eine ausführliche Störfallanalyse allerdings verzichtet, da stattdessen bereits krisenhafte Entwicklungstrends bei der Festlegung einiger Deskriptoren mitbedacht wurden.
Im Rahmen des Szenario-Transfers, des letzten Teilschrittes in der Phase der Szenario-Auswertung, wird eine Leitstrategie entwickelt und ein Umfeldbeobachtungssystem etabliert, um die bereits erarbeiteten Chancen und Risiken der Szenario-Beschreibungen nutzbar zu machen. Ziel des Szenario-Transfers ist es, auf Basis der bereits erarbeiteten Aktivitäten zu Chancen und Risiken eine Leitstrategie und eventuelle Alternativstrategien zu formulieren sowie ein Umfeldbeachtungssystem zu etablieren.

Der Untersuchungsgegenstand dieser Arbeit ist jedoch nicht die Formulierung von Strategien, um auf die Chancen und Risiken der jeweiligen Szenarien einzugehen. In der Szenario-Auswertung steht in dieser Arbeit die Beurteilung der rechtlichen Situation und Einschätzung der Gefahr der privaten Überwachung im Mittelpunkt. Die Zukunftsszenarien werden daher mit der aktuellen Rechtsprechung in Bezug gebracht, und auf ihre Umsetzbarkeit hin analysiert.

4 Szenarioentwicklung

Welche Einflussbereiche fördern oder hemmen die weitere Entwicklung und Verbreitung der RFID-Technologie und des Internets der Dinge bis ins Jahr 2020? Welche Faktoren sind dabei in den jeweiligen Einflussbereichen relevant, wie beeinflussen sich diese gegenseitig, und welche Ausprägung werden heutige Trends in der Zukunft haben?
Dieses Kapitel versucht, Antworten auf diese Fragen zu geben. Dazu werden zunächst die relevanten Einflussbereiche und deren Einflussfaktoren vorgestellt und auf ihre gegenseitige Beeinflussung hin überprüft. Es folgt eine Zukunftsprojektion abgeleiteter Deskriptoren, welche letztlich zu konsistenten Szenarien zusammengefasst werden.

4.1 Einflussbereiche und Einflussfaktoren

Die Identifikation und Beschreibung von Einflussfaktoren auf die zukünftige Entwicklung des Internets der Dinge stellt eine komplexe Aufgabe dar: So müssen psychologische, technische, soziale und ökonomische Faktoren beachtet werden, welche sich auch noch gegenseitig beeinflussen.

In den letzten Jahren wurden hierzu zahlreiche Positionspapiere und Studien von öffentlichen Informationsstellen, Verbänden und Forschungseinrichtungen veröffentlicht, welche fördernde und hemmende Faktoren für den zukünftigen Einsatz der RFID-Technologie und des Internets der Dinge beschreiben. Vier Studien wurden als empirische Grundlage dieser Arbeit ausgewertet: die Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ (2004) des BSI[64], welche ihre Erkenntnisse auf eine durchgeführte Expertenbefragung stützt, das Positionspapier „European Policy Outlook“ (2007) des BMWi[65], welches die Erkenntnisse aus einer Zusammenarbeit von Vertretern der Wirtschaft, der Verbände, der Regierungsorgane sowie der Europäischen Kommission zusammenfasst, die TAUCIS-Studie „Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung“ (2006) des ULD und der Humbold Universität[66], welche eine sehr wissenschaftliche Beschreibung von möglichen Bestimmungsfaktoren des Ubiquitous Computing liefert sowie der Forschungsbericht „Die IT- und Medienwelt in Baden-Württemberg im Jahr 2020“ (2008) der MFG Stiftung Baden-Württemberg[67], welcher sich auf eine Delphibefragung von Experten stützt. Basierend auf den Einschätzungen dieser vier Veröffentlichungen sowie durch eigene Überlegungen wurde eine Kategorisierung von Einflussbereichen für die zukünftige Entwicklung des Internet der Dinge hergeleitet (siehe Abbildung 5). Diese sei nun näher beschrieben:

---

[64] BSI (2004)

[65] BMWI (2007B)

[66] TAUCIS (2006)

[67] FAZIT-FORSCHUNG (2008)

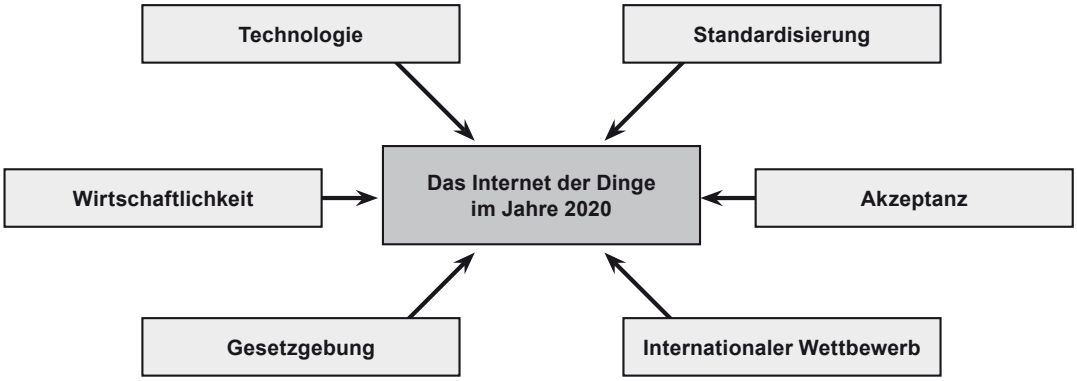

Abb. 5: Einflussbereiche auf das Internet der Dinge (eigene Darstellung)

Technologie: RFID als Basistechnologie des Internets der Dinge unterliegt derzeit noch technologischen Problemen, welche eine weitere Verbreitung hemmen. Darunter fallen etwa die Störanfälligkeit gegenüber Metall und Wasser oder auch die geringe Reichweite und das Problem der gleichzeitigen Erfassung von Gebilden. Die Größe der Transponder und der Lesegeräte muss weiter verkleinert werden, um neuartige Anwendungen zu ermöglichen. Integrierte Sicherheits- und Datenschutztechnologien müssen noch entwickelt werden. Erst wenn auch die Energieversorgung von aktiven Transpondern durch neue Technologien möglich wird, können Transponder mit Sensoren kombiniert werden, um die zweite Entwicklungsstufe des Internets der Dinge zu realisieren: das „Einander-bewusst-Machen" von Objekten und ihrer Umgebung. Die parallele Entwicklung von alternativen Technologien wie etwa der Lasertechnologie steht der Entwicklung der RFID-Technologie entgegen.

Standardisierung: Um ein branchen-, anwendungs- und länderübergreifendes Internet der Dinge zu etablieren, müssen einheitliche Standards definiert und eingeführt werden. Dabei spielt zum einen die weltweite Frequenzharmonisierung eine wichtige Rolle. Auf der anderen Seite müssen aber auch auf Anwendungsebene Standards beschrieben werden. Der EPC könnte sich dabei als ein Standard zur Objektkennzeichnung – nicht nur im Handel – herausstellen, und der ONS-Dienst könnte die Grundlage für eine neue technologische Infrastruktur zur Verknüpfung von Objekten mit dem Internet darstellen.

Wirtschaftlichkeit: Die Kennzeichnung von Produkten des täglichen Lebens mit RFID-Transpondern muss sich wirtschaftlich lohnen. Bevor die RFID-Technologie den Massenmarkt erreicht, müssen die Preise für Transponder deutlich günstiger werden. Auch die Kosten der Systemeinführung für Anwender, etwa durch neue Prozesse, Software und Hardware müssen dabei ebenfalls berücksichtigt werden. Schließlich beeinflusst auch das

Potenzial neuartiger Geschäftsmodelle im oder mit dem Internet der Dinge den weiteren Ausbau dieser Technologie.

Akzeptanz: Die Akzeptanz der Technologie bei professionellen Anwendern und Endverbrauchern stellt einen entscheidenden Einflussbereich dar. Gegenwärtige Datenschutzbedenken und Protestaktionen von Verbraucherschutzorganisationen belegen, dass die vielen neuen Möglichkeiten der Technologie nicht nur positiv aufgenommen werden. Die Akzeptanz hängt dabei von zahlreichen Faktoren ab. Die Einführungs- und Informationspolitik von Unternehmen und Politik wird ein wichtiger Faktor werden, wenn erste Anwendungen der RFID-Technologie im Endkundenbereich eingeführt werden. Die wahrgenommene Kontrolle über die übermittelten und erhobenen Daten sowie die Art ihrer Weiterverarbeitung werden entscheidend dazu beitragen, welches Vertrauen die Verbraucher der Technologie und ihren Betreibern entgegenbringen. Neuartige Anwendungen, welche einen deutlichen Nutzen stiften, indem sie die Arbeit effizienter oder bequemer machen, könnten die Akzeptanz dabei positiv beeinflussen und dazu beitragen, dass sich die Einstellung zur informationellen Selbstbestimmung in jüngeren Generationen verändern könnte. Ein Datenschutzskandal bei ersten Anwendungen könnte aber die Akzeptanz auch deutlich hemmen.

Gesetzgebung: In zwei Bereichen kann auch die Gesetzgebung die Entwicklung des Internets der Dinge beeinflussen. Durch Gesetze zum Schutze der Bürger und durch Umweltschutzgesetze. Wenn etwa Entsorgung und Wiederverwertung von Tags – im Sinne des Umweltschutzgesetzes – gesetzlich vorgeschrieben würden, könnten hohe Kosten für die Anwender entstehen, welche die weitere Verbreitung der Technologie stark bremsen würden.

Internationaler Wettbewerb: Europa steht im starken Wettbewerb zu Nordamerika und Asien. Die politische Relation zwischen den Nationen wird dabei entscheiden, wie stark es zu Kooperation oder Protektionismus kommen wird. Kooperation würde die Verbreitung von Standards und Infrastruktur fördern, Protektionismus hingegen würde die Verbreitung hemmen.

4.2 Vernetzungsmatrix

Wie bereits beschrieben, beeinflussen sich alle Einflussbereiche auch gegenseitig. In einer Vernetzungsmatrix kann nun herausgestellt werden, welche Einflussbereiche andere am stärksten beeinflussen. Sie werden durch eine hohe Aktivsumme in der Vernetzungsmatrix

deutlich. Durch eine hohe Passivsumme werden die Einflussbereiche deutlich, welche am stärksten von der Entwicklung anderer abhängig sind.[68]

In der folgenden Vernetzungsmatrix wird nun versucht, die gegenseitige Beeinflussung anhand einer Gewichtung zu beschreiben. Der Wert „0" bedeutet dabei keinen Einfluss, der Wert „1" beschreibt einen indirekten Einfluss und der Wert „2" beschreibt einen starken Einfluss. Die Werte in der folgenden Tabelle 2 basieren auf eigenen Überlegungen. Üblicherweise werden diese Werte durch eine Expertenbefragung ermittelt, welche im Rahmen dieser Arbeit jedoch nicht durchgeführt werden konnte.

	A Tech.	**B Stand.**	**C Wirtsch.**	**D Akzept.**	**E Gesetz.**	**F Wettb.**	**Aktivsumme**
A Technologie	X	1	2	2	1	2	**8**
B Standardisierung	1	X	2	2	1	1	6
C Wirtschaftlichkeit	2	2	X	2	2	1	**9**
D Akzeptanz	1	1	1	X	2	1	6
E Gesetzgebung	1	1	0	1	X	0	3
F Wettbewerb	0	1	0	1	1	X	3
Passivsumme	5	6	5	**8**	7	5	

Tab. 2: Vernetzungsmatrix (eigene Darstellung)

Eine Betrachtung der höchsten Werte in den Aktiv- und Passivsummen lassen nun folgende Interpretation zu: Die Einflussbereiche „Technologie" und „Wirtschaftlichkeit" haben den stärksten direkten Einfluss auf alle Bereiche. Die Einflussbereiche „Akzeptanz" und „Gesetzgebung" reagieren am stärksten auf eine Veränderung in den anderen Bereichen und haben damit den höchsten indirekten Einfluss. Die Ergebnisse erscheinen dem Verfasser plausibel.

4.3 Deskriptoren und Zukunftsprojektionen

Aus den oben beschriebenen Einflussbereichen und Faktoren wurden zusammenfassend 12 Deskriptoren für die weitere Szenariobildung abgeleitet (siehe Tabelle 3). Durch Hintergrundrecherche und eigene Überlegungen werden nun Projektionen der jeweiligen Deskriptoren in das Jahr 2020 vorgenommen. Zur klareren Nachvollziehbarkeit wird immer zuerst der jeweilige Ist-Zustand beschrieben. Die Zukunftsprojektionen werden durch Angabe der Hintergrundrecherche sowie durch eine Erläuterung der eigenen Überlegungen begründet.

[68] VON REIBNITZ, U. (1991), S. 35-37

Nr.	Einflussbereich	Deskriptor
D1	Technik	Überwindung aktueller technischer Probleme
D2		Entwicklung von Sicherheitstechniken
D3		Entwicklung adaptiver Systeme
D4	Standardisierung	Weltweite Frequenzharmonisierung
D5		Interoperationalität auf Anwendungsebene
D6	Wirtschaftlichkeit	Preisentwicklung von RFID-Systemen
D7		Wirtschaftliches Potenzial neuer Anwendungen
D8	Akzeptanz	Kontrollmöglichkeiten der Nutzer
D9		Nutzenempfindung und Technikgestaltung
D10		Einstellung zur individuellen Selbstbestimmung
D11	Gesetzgebung	Entwicklung von Gesetzen
D12	Int. Wettbewerb	Entwicklung des internationalen Wettbewerbs

Tab. 3: Zusammenfassung der Deskriptoren (eigene Darstellung)

4.3.1 Überwindung aktueller technischer Probleme

Ist-Situation	Technische Probleme bei RFID hemmen die weitere Verbreitung
Entwicklung A	Technische Probleme wurden überwiegend gelöst
Entwicklung B	Neue technische Probleme in der Polymertechnologie Lasertechnologie als Alternative zu RFID im Handel erfolgreich

Tab. 4: Deskriptor D1 (eigene Darstellung)

In diesem Deskriptor wird berücksichtigt, dass die aktuelle RFID-Technologie noch stärker entwickelt werden muss, bevor eine zuverlässige und effiziente Massenanwendung möglich werden kann. Die jetzigen Probleme liegen in der relativ geringen Reichweite von passiven Transpondern, in der hohen Störempfindlichkeit gegenüber Wasser und Metall sowie in der unzuverlässigen Erfassung von Gebinden, wenn mehrere Transponder gleichzeitig ausgelesen werden.[69]

Aufgrund der heute intensiven Forschung im Bereich der RFID-Technologie beschreibt Entwicklung A eine Situation, in der bis zum Jahre 2020 heutige technische Probleme gelöst werden konnten. Durch neue Antikollisionsprotokolle konnte die Leserate erhöht, und damit

[69] BSI (2004), S. 95

die Effektivität der RFID-Technologie deutlich verbessert werden.[70] Lesegeräte sind kleiner und vor allem sensibler geworden.

Nachfolgende Transponder-Generationen auf Polymerbasis sollen schon bald die heutigen Siliziumtransponder ersetzen, da sie in der Massenproduktion um 1/10 günstiger herzustellen sind.[71] Allerdings könnte die geringe Schaltgeschwindigkeit dieser Technologie neue Probleme mit sich bringen. Entwicklung B beschreibt eine Situation, in der zwar eine massenhafte Produktion von Transpondern zu günstigen Preisen möglich ist, aber neue technische Probleme einen breiten Einsatz der RFID-Technologie weiterhin hemmen. Stattdessen hat sich die Lasertechnologie zur Erfassung und Identifikation von Objekten im Handel durchgesetzt, da sie zwar weniger Informationen als die EAN-Technologie darstellen kann, jedoch aufgrund des erforderlichen Sichtkontaktes ein unerlaubtes Auslesen nicht ermöglicht.[72]

4.3.2 Entwicklung von Sicherheitstechniken

Ist-Situation	Sicherheitstechniken für Massenanwendungen noch undefiniert
Entwicklung A	Sicherheitstechniken sind ein zentrales Systemelement geworden
Entwicklung B	Sicherheitstechniken sind je nach Anwendungsbereich unterschiedlich stark ausgeprägt

Tab. 5: Deskriptor D2 (eigene Darstellung)

Nach Auffassung des BMWi wird die Frage der IT-Sicherheit in künftigen RFID-Systemen eine große Rolle spielen.[73] Zwar existieren bereits heute Sicherheits- und Datenschutztechniken gegen unerlaubtes Auslesen oder Manipulation der Daten auf den Transpondern (siehe Kapitel 2.2.3), aber sie sind noch nicht branchen- und anwendungsübergreifend etabliert und noch zu teuer für den Masseneinsatz. Das Fehlen von Sicherheitslösungen hemmt den Einsatz von RFID-Anwendungen gegenwärtig mehr als technische Probleme, da Unternehmen nicht die Gewissheit haben, dass Mitbewerber nicht auf vertrauliche Lieferkettendaten zugreifen können. Das BSI rechnet damit, dass erst in der nächsten Generation von RFID-Systemen Sicherheitstechniken stärker integriert sein

---

[70] BMWI (2007B), S. 25

[71] BMWI (2007B), S. 23

[72] RFID-BASIS.DE (2007), am 22.04.2009

[73] BMWI (2007B), S. 15, S. 28

werden.[74] Welche und ob überhaupt technische Sicherheits- und Datenschutzsysteme verwendet werden, wenn RFID den Endverbraucher erreichen wird, ist noch unklar.

Eine optimistische Möglichkeit wäre Entwicklung A, in der angenommen wird, dass Sicherheitstechniken zu einem zentralen Systemelement künftiger Informationstechnologien geworden sind. Schon jetzt sind sich Forschung, Politik und Unternehmen einig, dass eine Annahme und Nutzung der RFID-Technologie nur unter der Vorraussetzung einer sicheren Technologie erfolgen kann. Es kann also davon ausgegangen werden, dass in diesem Bereich noch große Fortschritte gemacht werden. In Zukunft könnte es vielleicht einen „Identitätsmanager" geben, einen elektronischen Helfer – beispielsweise integriert in neuen Mobiltelefonen – welcher die Rechteverwaltung von übermittelten Daten übernimmt.[75] Der Anwender könnte in seinem persönlichen Identitätsmanager zentral einstellen, welche Daten(spuren) er wo hinterlässt und gezielt mehr oder weniger Informationen ausgeben lassen. Zusätzlich könnte dieses Gerät seinen Benutzer auch warnen, wenn etwa ein unrechtmäßiger Lesezugriff erfolgt. In seiner kritischen Auseinandersetzung mit dem Thema „ Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing" (2007) bestätigt auch ROSSNAGEL[76], dass Selbstbestimmung nur dann eine Chance habe, wenn sie ebenfalls technisch unterstützt würde, und beschreibt dabei ebenfalls ein Gerät, welches automatisch die Rechteverwaltung für seinen Eigentümer übernimmt.

Ein weniger optimistisches Szenario beschreibt Entwicklung B, welche eher eine Fortführung der aktuellen Situation beschreibt. Dabei wird berücksichtigt, dass die Etablierung von branchenübergreifenden Sicherheits- und Datenschutztechniken ein hohes Maß an Standardisierung voraussetzt. Dieses ist jedoch schwierig zu realisieren, da je nach Anwendungsbereich unterschiedlich hohe Sicherheits- und Datenschutzanforderungen notwendig sind.[77] Für die Optimierung und Steuerung der eigenen Produktion werden innerhalb geschlossener Anwendungen in diesem Szenario nur noch sichere RFID-Systeme eingesetzt, zu hoch ist die Gefahr von Spionage und Manipulation. Allerdings wird in diesem Szenario nicht davon ausgegangen, dass auch Produkte des täglichen Lebens verschlüsselt werden. Vielmehr ist hier das Deaktivieren von Tags eine gängige Lösung geworden. Die bereits erfolgte Integration des „Kill-Tags" in EPC-kompabtiblen Transpondern ist ein Indiz für diese Annahme.

---

[74] BSI (2004), S. 99

[75] TAUCIS (2006), S. 137

[76] ROSSNAGEL, A. (2007), S. 281

[77] BMWI (2007B), S. 28

4.3.3 Entwicklung adaptiver Systeme

Ist-Situation	Technologie noch unausgereift
Entwicklung A	Breiter Einsatz von adaptiven Systemen
Entwicklung B	Adaptive Systeme sind Nischenanwendungen

Tab. 6: Deskriptor D3 (eigene Darstellung)

Wie das Internet der Dinge im Jahre 2020 aussehen wird, hängt auch maßgeblich davon ab, welche zusätzlichen Funktionen RFID-Systeme haben werden. Dieser Deskriptor fasst unter dem Begriff „Adaptive Systeme“ die Vorstellung von Objekten zusammen, welche, ausgestattet mit Sensoren und Mikrochips, intelligent auf ihre Umwelt reagieren können. Die Technologie für diese Vorstellung ist zurzeit noch nicht ausgereift. Sie muss kleiner werden, und vor allem muss das Problem der Energieversorgung gelöst werden, denn intelligente Objekte brauchen Energie[78].

Entwicklung A beschreibt ein Szenario, in dem Adaptive Systeme im breiten Einsatz sind. Durch Forschung auf dem Gebiet der Umgebungsenergie kann aus Bewegung, Temperaturwechsel oder Schall Energie gewonnen werden.[79] Batterien sind nicht mehr erforderlich. Die kleinen Helfer etablieren sich hier insbesondere durch nützliche neue Dienste immer mehr im Alltagsleben.

Entwicklung B geht davon aus, dass bis ins Jahr 2020 zwar Fortschritte auf dem Gebiet der Umgebungsenergie gemacht werden, dass aber deren Massenproduktion noch nicht wirtschaftlich ist. Dementsprechend sind adaptive Systeme noch Nischenanwendungen. In der Forschung werden aber bereits seit Jahren sogenannte Sensornetze eingesetzt, welche eine noch nie da gewesene Genauigkeit an Messdaten liefern.[80]

---

[78] BMWI (2007B), S. 22

[79] TAUCIS (2006), S. 66

[80] MATTERN, F. (2007), S. 15

4.3.4 Weltweite Frequenzharmonisierung

Ist-Situation	Ungeregelte weltweite Frequenzbereiche
Entwicklung A	Globale Frequenzharmonisierung erfolgreich
Entwicklung B	Frequenzharmonisierung auf europäischer Ebene erfolgreich

Tab. 7: Deskriptor D4 (eigene Darstellung)

Eine globale Frequenzharmonisierung sowie vereinfachte Zuweisungs- und Zulassungsverfahren werden nach Auffassung des BMWi die weitere Einführung von RFID-Anwendungen erleichtern.[81] Der Einsatz von RFID in internationalen Logistikketten und anderen für globale Märkte konzipierten Anwendungen erfordere eine einheitliche Verwaltung der Frequenzspektren. In den Bereichen Industrie, Wissenschaft und Medizin wurden bereits weltweit Frequenzen zugewiesen. In dem für Logistik und Handel wichtigen UHF-Bereich gibt es bis jetzt keine weltweit einheitlichen Bandbreiten. Die Europäische Kommission hat aber eine Entscheidung zur Harmonisierung der Frequenzbänder für RFID-Geräte im UHF-Bereich verabschiedet. Ob diese Entscheidung jedoch innerhalb der Mitgliedstaaten und später auch global zu einer Standardisierung führen wird, ist bis jetzt noch unklar.

Entwicklung A beschreibt ein Szenario, in dem eine globale Frequenzharmonisierung erfolgreich war. Unter dieser Annahme ist also ein derzeitiges Einführungshemmnis weltweit agierender Unternehmen überwunden worden, und es ist mit einer stärkeren globalen Verbreitung von RFID-Systemen im Jahr 2020 zu rechnen.

Auf der anderen Seite kann aber auch eine Situation eintreten, in der zwar auf europäischer Ebene eine Frequenzharmonisierung stattgefunden hat, jedoch keine globalen Frequenzstandards im UHF-Bereich existieren. Entwicklung B beschreibt diese Situation. Nach eigenen Überlegungen würde in diesem Falle die weltweite Verbreitung von RFID-Systemen gehemmt. Zwar ist davon auszugehen, dass es dann auch Lesegeräte geben wird, welche mehrere Standards verstehen (ähnlich den heutigen Mobiltelefonen), jedoch würden unterschiedliche Systeme zu höheren Kosten führen. Insgesamt sind in diesem Szenario weniger RFID-Systeme weltweit im Einsatz.

[81] BMWI (2007B), S. 17

4.3.5 Interoperationalität auf Anwendungsebene

Ist-Situation	Zahlreiche proprietäre, geschlossene Systeme, EPC und zahlreiche ISO-Standards beschreiben noch keine Standards auf Anwendungsebene
Entwicklung A	Interoperationalität durch branchenübergreifende Anwendungsstandards
Entwicklung B	Interoperationalität geprägt von nationalen und branchenabhängigen Rahmenbedingungen

Tab. 8: Deskriptor D5 (eigene Darstellung)

Die zentrale Frage, wie eine flexible Interaktion von Geräten, Softwareagenten und Diensten im Internet der Dinge sichergestellt werden kann, ist derzeit noch nicht gelöst. So gibt es zahlreiche proprietäre (geschlossene) Systeme und ISO-Standards auf technischer Ebene, jedoch ist eine Interoperationalität, als Grundvoraussetzung eines offenen Systems, derzeit noch nicht möglich. Auf Anwendungsebene fehlen die notwendigen Standards, um ein Internet der Dinge zu ermöglichen. Eine Anwenderbefragung des BSI bestätigt, dass das Fehlen von Standards aus ökonomischer Perspektive ein vorrangiges Hindernis für neue Anwender der RFID-Technologie darstellt.[82] Nach Auffassung des BMWi sind für den globalen und unternehmensübergreifenden Austausch von Daten RFID-gekennzeichneter Objekte die Spezifizierung und Verfügbarkeit von drei Komponenten erforderlich: der Daten auf dem Chip, einer Suchfunktion für angeschlossene Anwendungen sowie der zeit- und ortsbezogenen Aggregation und Interpretation dieser objektbezogenen Daten. Das von EPCglobal konzipierte EPC-Netz (siehe auch Kapitel 2.1.2) würde eine Möglichkeit zur Umsetzung dieser drei Aspekte darstellen.[83] Es ist aber derzeit noch nicht in Betrieb.

Entwicklung A beschreibt nun ein Szenario, in dem das EPC-Netzwerk zum allgemeinen, globalen Standard geworden ist. Auf allen Transpondern ist die eindeutige EPC-konforme Identifikationsnummer enthalten. Über den ONS-Dienst können nun auch Objekte im Internet eindeutig adressiert und gefunden werden. Die Vision vom Internet der Dinge ist damit Realität geworden, und zahlreiche neue Anwendungen haben sich darum herum entwickelt. Durch die starke Verbreitung des EPC-Standards sind auch zahlreiche – zunächst proprietäre – Branchenlösungen auf diesen Standard umgestiegen, sodass nun auch ein branchenübergreifender Datenaustausch stattfinden kann.

Entwicklung B beschreibt eine Situation, in der mehrere Faktoren dazu geführt haben, dass das EPC-Netzwerk in Europa nicht zur Grundlage eines interoperationalen Netzwerkes

[82] BSI (2004), S. 97

[83] BMWI (2007B) S. 26, 27

geworden ist. Ein Faktor, der diese Entwicklung befürworten würde, wäre beispielsweise die Befürchtung der Europäischen Kommission, dass das EPC-Netzwerk nicht der europäischen Rechtsprechung unterliegen könnte und somit eine Missbrauchsgefahr für Bürger und Wirtschaft existieren würde.[84] Ein anderer Faktor, der dazu führen könnte, dass sich das EPC-Netzwerk nicht im geplanten Umfang und branchenübergreifend entwickeln könnte sind Patente. Einige Unternehmen könnten sich ihre speziellen Branchenlösungen oder auch Technologien patentieren lassen, was eine Standardisierung hemmen würde. Hinzu kommt, dass eine Abhängigkeit von US-amerikanischen Patenteinhabern nicht im Interesse der europäischen Wirtschaft läge. In diesem Szenario wird angenommen, dass das EPC-Netzwerk sich in Amerika durchgesetzt hat. In Europa hat sich ein eigener, interoperabler Dienst nach dem Vorbild des EPC-ONS-Dienstes entwickelt, welcher in einigen Bereichen auch kompatibel mit dem EPC-Netzwerk ist. Der Datenaustausch und die Interoperationalität sind in diesem Szenario also stark branchenabhängig. Innerhalb der Branchen haben sich aus zahlreichen proprietären Lösungen Branchenstandards entwickelt. Das Internet der Dinge ist in diesem Szenario im Jahre 2020 zusammenfassend stark von nationalen und branchenabhängigen Rahmenbedingungen geprägt. Dadurch sind viele Visionen möglicher Anwendungen nicht oder nur eingeschränkt möglich geworden.

4.3.6 Preisentwicklung von RFID-Systemen

Ist-Situation	Technologie ist für den Massenmarkt noch zu teuer
Entwicklung A	Technologiepreise und Einführungskosten sind rapide gesunken
Entwicklung B	Einführungskosten sind durch die neue Komplexität hoch geblieben

Tab. 9: Deskriptor D6 (eigene Darstellung)

In einer wirtschaftlichen Analyse von Kosten und Nutzen der RFID-Technologie identifiziert MAREK[85] zwei grundsätzliche Kostenarten: die Hardwarekosten, bestehend aus den benötigten Transpondern, Lesegeräten und Netzwerken, sowie die Integrations- und Folgekosten, bestehend aus der Reorganisation von Geschäftsprozessen, der Software und der Systemwartung. Beide Kostenarten sind nach Einschätzung aller vorliegenden Studien gegenwärtig noch zu hoch. Die Transponder auf Siliziumbasis können noch nicht zu einem

[84] BMWI (2007B), S. 19

[85] MAREK, C. (2007), S. 16

Stückpreis produziert werden, der für den Massenmarkt günstiger Produkte geeignet ist. Das Fehlen von standardisierten Branchenlösungen führt dazu, dass sich die Einführung der RFID-Technologie für zahlreiche kleine und mittelständische Unternehmen noch nicht lohnt.[86]

Entwicklung A beschreibt auch hier wieder eine positive Entwicklung. Unter der Annahme, dass sich Anwendungsstandards etablieren konnten, sind die Integrationskosten für Anwender stark gesunken. Unternehmen können jetzt auf ein großes Angebot an Standardlösungen zurückgreifen. Neuartige Transpondergenerationen, basierend auf der oben bereits beschriebenen Polymertechnologie, haben dazu geführt, dass nun auch die Kennzeichnung von Massenartikeln mit RFID-Technologie wirtschaftlich geworden ist. Eine weitere mögliche Begründung für dieses Szenario liefert das Gesetz von Moore, nach dem sich alle anderthalb Jahre die Leistungsfähigkeit von Prozessoren verdoppeln und zudem die Preise und die Größe sinken.[87]

Entwicklung B geht unter der Annahme fehlender globaler und branchenübergreifender Anwendungsstandards davon aus, dass die Integrationskosten für RFID-Systeme weiterhin hoch geblieben sind. Die neuen Möglichkeiten der RFID-Technologie in Produktion und Automatisierung haben zu einer neuen Komplexität in der Systemintegration geführt, und Anwendungen sind damit teure Individuallösungen geblieben. Die Hardwarekosten hingegen sind auch in diesem Szenario deutlich gesunken. Zwar konnten die neuen Polymertransponder noch nicht in einer ausreichenden Leistungsfähigkeit für den Massenmarkt produziert werden, aber die Stückpreise für Transponder auf Siliziumbasis sind deutlich unter einen Cent gesunken. Um die Integrationskosten dennoch für kleinere und mittelständische Unternehmen zu senken, haben große Konzerne ihre Lieferanten motiviert, RFID-Lösungen nach ihren Systemanforderungen einzusetzen. Diese Strategie fahren Wal-Mart, Metro und Tesco bereits seit mehreren Jahren. [88]

---

[86] BSI (2004), S. 97

[87] MATTERN, F. (2005), S. 42-44

[88] KNEBEL, U.; LEIMEISTER, J. M.; KRCMAR, H. (2007), S. 1

4.3.7 Wirtschaftliches Potenzial neuer Anwendungen

Ist-Situation	Potenzial in Logistik und Lieferketten, Angebote im privaten Bereich noch nicht vorhanden
Entwicklung A	Großes wirtschaftliches Potenzial im privaten- und gewerblichen Bereich
Entwicklung B	Großes wirtschaftliches Potenzial im gewerblichen Bereich, wenig im privaten Bereich

Tab. 10: Deskriptor D7 (eigene Darstellung)

Die zahlreichen Visionen möglicher Anwendungen für das Internet der Dinge können nur dann zur Realität werden, wenn es auch eine wirtschaftliche Motivation für ihre Entwicklung und ihren Betrieb gibt. Plakativ formuliert stellt sich also die Frage, wer womit im Internet der Dinge Geld verdienen wird. HASENKAMP[89] beschreibt in diesem Zusammenhang, dass das Erreichen einer kritischen Masse von Anwendern, insbesondere auch im privaten Bereich, zu einer kostengünstigen Massenfertigung von Geräten sowie zu einem wirtschaftlichen Betrieb der erforderlichen Infrastruktur führen würde. Gegenwärtig entfaltet die RFID-Technologie ihr Potenzial besonders bei der Effizienzsteigerung in der Logistik und in Lieferketten. Eine Kategorisierung von betriebswirtschaftlichen Nutzenpotenzialen des Internets der Dinge (hier „UbiComp“ genannt für Ubiquitous Computing) liefern FLEISCH, MATTERN UND BILLINGER[90] (siehe Tabelle).

Nutzenpotenziale	**Intern**	**Extern**	
	Organisationspotenzial	Informatik- und Technologiepotenzial	
	Kostensenkungspotenzial	Finanzpotenzial	
	Know-how-Potenzial	Beschaffungspotenzial	
Strategische Erfolgspositionen	**Qualität**	**Leistungsbreite**	**Innovationen**
	Produkt	Dienstleistungen	Technologie
	Prozess	Leistungssysteme	Trendsetting
Resultate	Effizienzsteigerung		Effektivitätsteigerung
Themenbereiche der UbiComp	Operative Leistungssteigerung	Services	Neue Produkte

Tab. 11: Themenbereiche und Resultate des Internets der Dinge nach FLEISCH ET AL.

Sie sehen die Möglichkeiten der Effizienz- und Effektivitätssteigerung der neuen Technologien als Auslöser für neue Anwendungen, welche zu einer operativen

[89] HASENKAMP, U. (2008), S. 110

[90] FLEISCH, E., MATTERN, F., BILLINGER, S. (2004) S. 10

Leistungssteigerung, zu neuen Services und zu neuen Produkten führen können. Welche Anwendungen im privaten Bereich konkret eine Nachfrage erzeugen könnten und wie sich daraus Geld verdienen ließe, wird in der ausgewerteten Literatur jedoch kaum beschrieben. Aus diesem Grunde beschreibt dieser Deskriptor nicht konkrete Anwendungen sondern versucht vielmehr die Auswirkungen zu beschreiben, wenn neue Anwendungen eine Nachfrage erzeugen oder eben nicht.

Entwicklung A beschreibt ein Szenario, in dem sukzessive neue Anwendungen – insbesondere auch im privaten Bereich – gefunden wurden, deren Betrieb sich auch wirtschaftlich lohnt. In diesem Szenario wird weiterhin davon ausgegangen, dass diese Anwendungen auch auf eine hohe Akzeptanz gestoßen sind, einem weiteren Einflussbereich, der im nächsten Deskriptor ausführlicher behandelt wird. Unter diesen Annahmen hat sich das Internet der Dinge im Jahre 2020 stark entwickelt und ist auch in den privaten Haushalten angekommen. Es haben sich zahlreiche neue Produkte und Dienstleistungen rund um das Internet der Dinge gebildet. Unternehmen investieren stark in die Weiterentwicklung der zugrunde liegenden Technologien. Insgesamt sind dadurch auch die Systemkosten stark gesunken. Die Ortung von Objekten ist nun über eingebaute GPS-Empfänger in den Transpondern selbstverständlich geworden. Dadurch hat sich der Diebstahl von teuren Produkten stark reduziert. Durch eingebaute Sensoren mit eigener Energiequelle sind intelligente Umgebungen möglich geworden, welche sich auf die Objekte in ihrer Nähe anpassen können. Zahlreiche Geschäftsprozesse laufen nun vollautomatisch ab, da die Objekte nun auch in der Lage sind, eigenständige Entscheidungen zu treffen. Einige dieser intelligenten Objekte wurden als „Gebrauchsmuster“ von Unternehmen geschützt und werden nun gewinnbringend lizenziert. Um das Internet der Dinge ist ein neuer, bedeutender Wirtschaftsbereich entstanden.

Entwicklung B beschreibt ein Szenario, in dem zwar zahlreiche Anwendungen im Endkundenbereich getestet worden sind, jedoch, vergleichbar mit der Situation zahlreicher heutiger Online-Startups, die Nutzer nicht bereit waren, für diese neuen Dienste Geld zu bezahlen. Zudem haben die Befürchtungen vieler Verbraucher, auf Schritt und Tritt von Staat und Unternehmen überwacht zu werden, zu einer bewussten Technologie-Verweigerung geführt. Ein entsprechender Entwicklungspfad wird beispielsweise im EPIS-Report 2008 beschrieben.[91] In diesem Szenario hat das Internet der Dinge durch die fehlende wirtschaftliche Motivation der Anbieter, Anwendungen zu betreiben, nicht den privaten

[91] EPIS-Report (2008), S. 33ff.

Endverbraucher erreicht. Das Internet der Dinge hat sich in der gewerblichen Nutzung jedoch als sinnvoll erwiesen und ist in diesem Szenario stärker auf Geschäftskunden ausgerichtet. Durch neue technische Möglichkeiten konnten Unternehmen Dienste bereitstellen, welche ihnen neue ökonomische Potenziale eröffneten, jedoch aus Verbrauchersicht nicht unbedingt wünschenswert sind.[92] So werden zahlreiche Leistungen, wie etwa die Entsorgung des Hausmülls, jetzt nach Nutzungsintensität abgerechnet. Wenn man von der Entwicklung des heutigen Internets Rückschlüsse auf die Entwicklung des Internets der Dinge zieht, könnte es in diesem Szenario auch passieren, dass die private Nutzung zu einem späteren Zeitpunkt noch erfolgen wird. Kommerzielle Angebote für private Nutzer wurden im Internet auch erst in den letzten Jahren stärker angenommen. Auch hier war am Anfang die Angst vor Manipulation und fehlender Sicherheit bei Zahlvorgängen ein hemmender Faktor für die zahlreichen Online-Shops.

4.3.8 Kontrollmöglichkeiten der Nutzer

Ist-Situation	RFID-Systeme sind noch nicht im Endkundenbereich
Entwicklung A	Wahlmöglichkeiten für Nutzer, transparente Technologieeinführung
Entwicklung B	Keine Wahlmöglichkeiten der Technologienutzung

Tab. 12: Deskriptor D8 (eigene Darstellung)

Neben den beschriebenen technischen und wirtschaftlichen Faktoren hängt die zukünftige Verbreitung der RFID-Technologie, und damit auch die des Internets der Dinge, maßgeblich von der Akzeptanz der Technologie und der Anwendungen bei den Endkunden ab. Da bisher nur wenig Anwendungen im Endkundenbereich eingesetzt werden, lässt dieser Deskriptor einen weiten Raum für mögliche Entwicklungsrichtungen zu. SPIEKERMANN ET AL.[93] liefern in diesem Zusammenhang ein Modell sozialer und psychologischer Akzeptanzfaktoren (siehe Abbildung 6), welches die Grundlage der weiteren Überlegungen darstellt. Neben der vom Nutzer empfundenen Nützlichkeit neuer Dienste entscheiden sein Vertrauen in den Anbieter und die wahrgenommene Kontrolle über die Technologie darüber, ob ein Dienst angenommen oder abgelehnt wird.

---

[92] TAUCIS (2006), S. 90

[93] SPIEKERMANN, S., ROTHENSEE, M.: (2005), S. 10

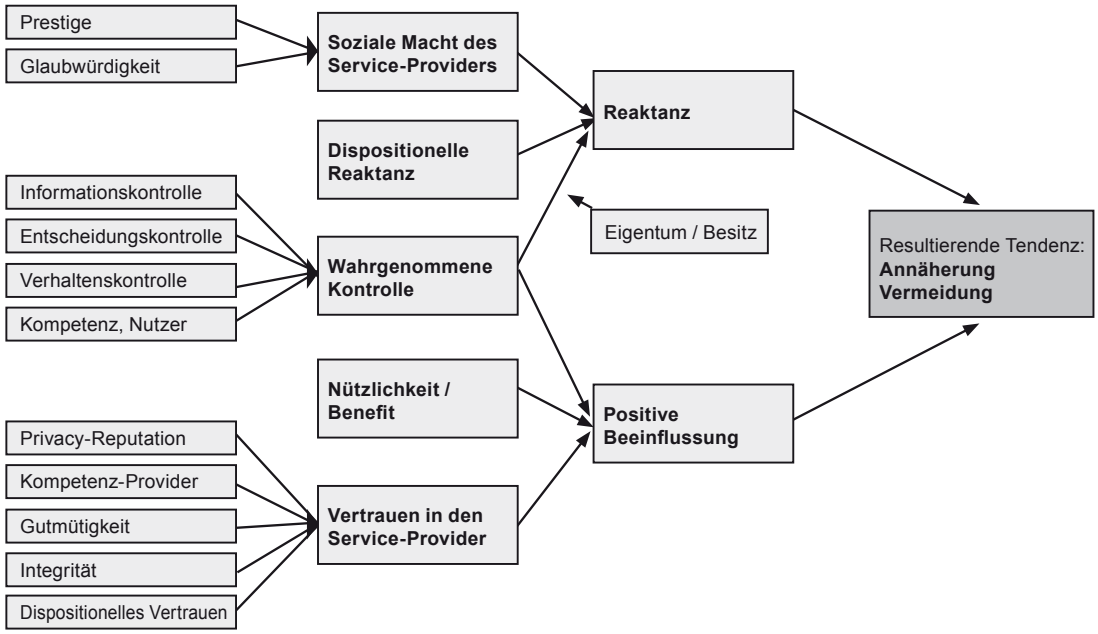

Abb. 6: Bestimmungsfaktoren des Ubiquitous Computing nach SPIEKERMANN

Die beiden letztgenannten Faktoren hängen in der Markteinführung neuer Anwendungen unmittelbar zusammen und werden in diesem Deskriptor näher betrachtet. Die Nützlichkeit neuer Anwendungen, als weiterer Akzeptanzfaktor, wird im hierauf folgenden Deskriptor behandelt.

In Entwicklung A wird wieder eine positive Situation beschrieben, in der das Verhalten der Anbieter bei der Markteinführung neuer Anwendungen mit RFID-Technologie zu einer verstärkt wahrgenommenen Kontrolle durch die Nutzer geführt hat. Die überwiegende Zahl an Nutzern vertraut den Anbietern. Zunächst wurde mit großen Plakaten innerhalb der Läden über den Einsatz der RFID-Technologie aufgeklärt. Im Handel konnten die Kunden in der frühen Markteinführungsphase weiterhin Produkte ohne Tags kaufen oder sämtliche Tags deaktivieren, was sowohl softwareseitig als auch durch ein manuelles Zerstören der Transponder ermöglicht wurde. Alle Produkte mit Tags wurden entsprechend gekennzeichnet.[94] Die zunehmenden neuen Anwendungen und Endgeräte für Datensicherheit (wie oben beschrieben) haben jedoch dazu geführt, dass immer weniger Tags freiwillig zerstört wurden. Die Nutzer haben hier stets die Wahl, ob sie sogenannte „intelligente Dienste“, wie etwa den persönlichen Einkaufsberater oder die nutzungs- und verhaltensabhängige Autoversicherung, in Anspruch nehmen wollen oder nicht. Den

[94] BMWI (2007A), S. 22

Anbietern war seit Beginn der Markteinführung RFID-basierter Dienste bewusst, dass nur eine transparente Informationspolitik zu einem Vertrauen der Nutzer und letztlich zu einer Akzeptanz der Dienste führen würde. In diesem Szenario ist die Technologie daher auf breiter Front akzeptiert.

Eine mögliche ablehnende Haltung wird im Akzeptanzmodell mit dem Begriff der dispositionellen Reaktanz beschrieben, welche wie folgt definiert wird: „*Die Reaktion von Individuen hin zur Wiederherstellung von Freiheiten, wenn diese Freiheiten bedroht oder eliminiert wurden.*“[95] Entwicklung B beschreibt ein Szenario, in dem diese ablehnende Haltung seit der Markteinführung von Anwendungen im Endkundenbereich dominiert. SPIEKERMANN hält eine solche Entwicklung dann für möglich, wenn dem Nutzer keine Wahlmöglichkeit gelassen wird, ob und wie die Technologie angewendet wird oder nicht. Dabei sei es auch irrelevant, ob der Nutzer Funktionen deaktivieren könne oder nicht.[96]

Wohl wissend, dass die möglichen Beobachtungsgefahren von RFID-Systemen vielen Menschen nicht bewusst oder schlicht egal sind (da sie nicht als mögliche Bedrohung eingestuft werden[97]), haben viele Unternehmen die Technologie eingeführt, ohne die Nutzer entsprechend aufzuklären. Aus Kostengründen wurden auch keine Wahlmöglichkeiten bei der Technologienutzung oder etwa die Alternative der Vermeidung geschaffen. Dies hat zu einer Abwehrhaltung der Kunden geführt. Im Jahre 2020 werden daher wieder viele Produkte ohne RFID-Kennzeichnung verkauft.

---

[95] BREHM, S., BREHM, J. (1981)

[96] SPIEKERMANN, S., ROTHENSEE, M. (2005), S. 11

[97] SPIEKERMANN, S., ROTHENSEE, M.(2005), S. 8

4.3.9 Nutzenempfindung und Technikgestaltung

Ist-Situation	Einige Anwendungen stellen einen hohen Nutzen dar und sind dadurch akzeptiert
Entwicklung A	Der Nutzen zahlreicher neuer Anwendungen wird überwiegend als hoch empfunden
Entwicklung B	Der Nutzen neuer Anwendungen wird überwiegend als niedrig empfunden

Tab. 13: Deskriptor D9 (eigene Darstellung)

Durch eine ganze Reihe von Studien in den USA wurde in den letzten 15 Jahren das so genannte „Technologieakzeptanzmodell“ nachgewiesen, welches die wahrgenommene Nützlichkeit einer Technologie neben deren Einfachheit (in der Bedienung) als den wichtigsten Faktor für ihre nachhaltige Adaption postuliert.[98] In diesem Zusammenhang kann ein hoher empfundener Nutzen einer Technologie auch ihre potenziellen Gefahren, etwa für die individuelle Selbstbestimmung, aufwiegen. LANGHEINRICH[99] belegt dieses Phänomen am Beispiel des Mobilfunks: Der Vorteil, schnell und unkompliziert überall und jederzeit Termine umzudisponieren bzw. Auskünfte einholen zu können, wöge für viele Nutzer die Nachteile einer potenziellen Überwachung mehr als auf. Gleiches gelte auch für Kreditkarten und Kundenkarten, welche detaillierte Einblicke in das Kauf- und Bewegungsverhalten erlaubten: Der Vorteil des bargeldlosen Bezahlens oder Rabatte durch das Nutzen von Kundenkarten wögen Datenschutzbedenken auf. Zusammenfassend beschreibt LANGHEINRICH[100] ein Spannungsfeld zwischen Datenschutz und Privatsphäre auf der einen und wirtschaftlicher Effizienz, persönlicher Bequemlichkeit sowie allgemeiner Sicherheit auf der anderen Seite. Obwohl im Zusammenhang mit der RFID-Technologie stets auch das Risiko der Überwachung thematisiert wird, sind elektronische Skipässe, Bezahlsysteme für Veranstaltungen und Nahverkehr sowie die elektronische Wegfahrsperre auf Basis dieser Technologie akzeptiert. Der Nutzen und die Einfachheit überwiegen demnach die empfundene Bedrohung einer möglichen Überwachung.

Es stellt sich also die Frage, ob wir die künftigen Anwendungen mit einem hohen Nutzen verbinden werden und ob wir bereit sind, „soziale Kosten“ in Form des Verlustes an informationeller Selbstbestimmung oder einer technischen Bevormundung dafür zu tragen.

Entwicklung A beschreibt eine Situation, in der die Menschen im Jahre 2020 einen hohen Nutzen in neuen Anwendungen sehen. Die zahlreichen neuen technischen Möglichkeiten,

---

[98] TAUCIS (2006), S. 157 mit Bezug auf VENKATESH (2000) und DAVIS (1989)

[99] LANGHEINRICH, M. (2008), S. 21

[100] LANGHEINRICH, M. (2007), S. 253

etwa der persönliche Einkaufsberater in der Umkleide (auf Grundlage eines Kundenprofils), die automatisch generierten Bestelllisten von elektronischen Haushaltshilfen oder die vollautomatischen Zugangssysteme für Büro und Eigenheim möchte man nicht mehr missen, da sie einem viel Zeit sparen. Ältere Menschen und Menschen mit einer Behinderung schätzen die Hilfestellungen, welche die neuen Technologien ihnen bieten.
Entwicklung B beschreibt eine Situation, in der zwar einige neue Anwendungen im Einsatz sind, die elektronischen Helfer aber Nischenanwendungen darstellen. Zwar gibt es Kühlschränke, welche automatisch Produkte nachbestellen können, jedoch haben sich nur wenige Käufer gefunden, die für diese zusätzliche Funktion Geld bezahlen wollten. Eine mit 8.000 Teilnehmern durchgeführte Verbraucherstudie des Instituts für Wirtschaftsinformatik der Humboldt-Universität zu Berlin in Kooperation mit der Wochenzeitung DIE ZEIT bestätigt diese Einschätzung: Der intelligente Kühlschrank wird zwar als „eher nützlich“ und „einfach“ in der Bedienung angesehen, jedoch wird die Kaufintention als „eher negativ“ angegeben. Gleiches gilt auch für andere beispielhafte Anwendungen, welche im Rahmen dieser Studie untersucht worden sind.[101] Ingesamt ist der persönliche Kontakt den Menschen wieder wichtiger geworden, was dazu geführt hat, dass wieder mehr echte Einkaufsberater engagiert wurden. Verbunden mit der Angst vor der persönlichen Überwachung durch Staat oder Unternehmen, aber auch durch Kriminelle, stehen die Menschen in diesem Szenario den Visionen des Internets der Dinge skeptisch gegenüber.

4.3.10 Einstellung zur individuellen Selbstbestimmung

Ist-Situation	Tendenz in der jüngeren Generation Richtung mehr Offenheit
Entwicklung A	Einstellung hat sich weiter in Richtung Offenheit gewandelt
Entwicklung B	Einstellung hat sich zurück zu mehr Privatheit gewandelt

Tab. 14: Deskriptor Frequenzharmonisierung (eigene Darstellung)

Die Einstellung zur individuellen Selbstbestimmung ist ein weiterer Faktor, der die Akzeptanz des Internets der Dinge und der darauf basierenden Anwendungen beeinflussen wird. Betrachtet man heutzutage das Verhalten insbesondere jüngerer Generationen, scheint sich die Einstellung zur individuellen Selbstbestimmung gewandelt zu haben – so werden freiwillig

[101] TAUCIS (2006), S. 159-161

immer mehr persönliche Daten digitalisiert und weltweit erfassbar gemacht:[102] In öffentlichen Blogs diskutieren Menschen ihre politische Meinung, mittels Twitter-Diensten werden minutengenaue Statusberichte der persönlichen Gefühlslage oder einer Beschreibung der Situation, in der man sich gerade befindet, an die Öffentlichkeit kommuniziert. In Communities werden Freundschaftsnetzwerke und private Fotos zusammen mit zahlreichen Angaben über Vorlieben und Einstellungen mit der Öffentlichkeit geteilt. LANTERMANN[103] beschreibt diese Tendenz als Bedürfnis nach Kontrollverlust, ein „heimliches" (?) Anwachsen der Befriedigung des Bedürfnisses nach Sozialität.

Entwicklung A beschreibt hier ein Szenario, in dem dieses Bedürfnis nach Sozialität gewachsen ist. In der Einstellung zur individuellen Selbstbestimmung ist hier ein weiterer Wandel in Richtung Offenheit erfolgt. Einen Beleg für diese Annahme könnte ein historischer Rückblick geben: Sowohl bei der Erfindung der Fotografie als auch bei der zunehmenden Verbreitung des Internets wurden stets auch Befürchtungen laut, dass diese neuen Technologien einen großen Eingriff in die individuelle Selbstbestimmung darstellen würden. Dennoch sind diese Technologien heutzutage allgemein akzeptiert. Entsprechendes gilt in diesem Szenario auch für die Einstellung zu Objekten, welche mit einer eindeutigen Identifikationsnummer versehen sind und somit grundsätzlich mit ihrem Eigentümer in Verbindung gebracht werden könnten. Sie sind selbstverständlich geworden. Eine Begründung dieser Annahme liefert beispielsweise auch LANTERMANN, der davon ausgeht, dass sich im Laufe der Zeit beides ändert – die Gesellschaft und die Technologie.[104] Auch LANGHEINRICH[105] thematisiert in diesem Zusammenhang einen Wandel der *gefühlten* Privatheit, und der Bundesbeauftragte für Datenschutz, SCHAAR[106], stellt allgemein fest, dass Privatangelegenheiten heute weitaus freizügiger öffentlich gemacht werden.

Auf der anderen Seite könnte sich aber auch genau das Gegenteil einstellen: Durch negative Erlebnisse im Internet, etwa dadurch, dass grundsätzlich jeder Mensch heutzutage „gegoogelt" werden kann und seine Geschichte somit allen zugänglich ist, könnte sich die Einstellung zur individuellen Selbstbestimmung zukünftig auch wieder in Richtung von mehr Privatheit entwickeln. In diesem Falle wäre die Akzeptanz zahlreicher Anwendungen im Internet der Dinge zunächst vakant, Datenschutztechnologien würden an Bedeutung

---

[102] LANGHEINRICH (2007), S. 245

[103] LANTERMANN, E. (2008), S. 190

[104] LANTERMANN, E. (2008), S. 185

[105] LANGHEINRICH (2007), S. 245

[106] SCHAAR, P. (2007), S. 18

gewinnen. Entwicklung B beschreibt eine Zukunft, in der den Menschen ihre Privatheit wieder wichtiger geworden ist. Sowohl der – bereits beschriebene – EPIS-Report 2008 als auch die FAZIT-Studie beschreiben beide ein entsprechendes Szenario. Die Rückbesinnung auf mehr Privatheit könnte aber auch durch einen Datenskandal ausgelöst werden. Derzeit sind zahlreiche Berichte in den Medien, welche über Unternehmen berichten, die ihre Mitarbeiter überwachen, wie aktuell etwa die Deutsche Telekom[107]. Sollte bekannt werden, dass Unternehmen auch Informationen über das Einkaufsverhalten ihrer Kunden, welches heute bereits durch Kundenkarten erfassbar ist, unrechtmäßig nutzen, dann würde dies die Einstellung zur Hinterlassung von Daten in der Öffentlichkeit mit Sicherheit stark beeinflussen. In diesem Szenario wird unterstellt, dass dieser Fall eingetreten ist. Das Bedürfnis nach mehr Privatheit hat sich infolgedessen wieder stark erhöht.

4.3.11 Entwicklung von Gesetzen

Ist-Situation	Gesetzesänderung für Datenschutz wurde geprüft und abgelehnt
Entwicklung A	Gesetzeslage hat sich der Technologie angepasst
Entwicklung B	Störereignis: Umweltschutzgesetz

Tab. 15: Deskriptor D11 (eigene Darstellung)

Neben der Frequenzregulierung unterliegen zwei weitere Bereiche der staatlichen Aufsicht, wenn es um die weitere Verbreitung der RFID-Technologie geht: Werden personenbezogene oder personenbeziehbare Daten per Funk übermittelt, müssen die Belange des Datenschutzes beachtet werden. Relevant ist hier die Datenschutzrichtlinie 95/46/EG des Europäischen Rates, welche eine verbindliche Regelung zum Schutz persönlicher Daten bei der Datenverarbeitung vorschreibt. Sie wurde von den Mitgliedstaaten in nationales Recht umgesetzt und ist somit Bestandteil des Bundesdatenschutzgesetztes. Nach einem Bericht des Bundesministeriums des Inneren[108] sieht die Bundesregierung derzeitig hier keinen gesetzlichen Handlungsbedarf. Die Rechte zum Schutze der Bürgen seien durch das Bundesdatenschutzgesetz ausreichend gesichert.
Aufgrund der Materialzusammensetzung von RFID-Transpondern spielen aber auch umweltpolitische Regularien eine zunehmend wichtige Rolle, wenn zukünftig Transponder in

[107] SPIEGEL.DE (2008), am 22.04.2009

[108] BMI (2008), S. 15

Alltagsgegenstände integriert und wieder entsorgt werden müssen.[109] Nach einer Einschätzung des BMWi stellt die Verbrennung von Transpondern wegen ihrer chemischen Zusammensetzung kein Problem dar. Die Schwierigkeiten lägen jedoch in Recycling-Prozessen. Es bestünde die Gefahr, dass durch die integrierten Kupfer, und Silizium-Stoffe andere Recycling-Güter wie Glas, Aluminium oder Papier verunreinigt würden, wenn Transponder in Massenanwendungen eingesetzt werden.[110]

Entwicklung A beschreibt ein Szenario, in dem sich die europäische Gesetzeslage im Jahre 2020 an die neuen technologischen Möglichkeiten angepasst hat und einen positiven Rahmen für ihren reibungslosen Einsatz darstellt. Die Notwendigkeit für diese Annahme beschreibt das BMWi in seinem Positionspapier zur Expertenkonferenz im Rahmen der deutschen EU-Ratspräsidentschaft. So wird empfohlen, die Datenschutzgesetze regelmäßig auf ihre Eignung für die stark zunehmende Vernetzung von ITK-Systemen [...] zu überprüfen und gegebenenfalls im Sinne einer nachsorgenden Regulierung an neue Erfordernisse anzupassen.[111] In diesem Szenario ist beispielsweise, wie bereits aktuell im US-Bundesstaat Washington erfolgt, das heimliche Auslesen von RFID-Tags gesetzlich verboten worden.[112] Insgesamt haben eine Reihe neuer Gesetze in diesem Szenario die Einführung und Verbreitung des Internets der Dinge eher gefördert. Die Gesetzgebung kann sich jedoch auch hemmend auf die weitere Entwicklung des Internets der Dinge auswirken, wie in Entwicklung B illustriert wird. Ein Störereignis in Form eines angekündigten neuen Umweltschutzgesetzes könnte hier dazu führen, dass das Anbringen von RFID-Transpondern auf recyclingfähigen Produkten verboten wird. Wie bereits oben beschrieben, gibt es bereits heute entsprechende Einschätzungen, dass die Wiederverwertung von getagten Produkten ein Problem darstellen könnte. Ein anderes Störereignis könnte auch ein Gesetz zum Schutze der Gesundheit darstellen, wenn etwa nachgewiesen würde, dass die erhöhte Funkstrahlenbelastung durch die neuen Technologien ein Gesundheitsrisiko darstellt.

---

[109] BMWI (2007B), S. 21

[110] BMWI (2007B), S. 25

[111] BMWI (2007B), S. 44

[112] INFORMATIONWEEK.COM (2008) am 22.04.2009

4.3.12 Entwicklung des internationalen Wettbewerbes

Ist-Situation	Die intensive Forschung in Asien und Amerika steht in starkem Wettbewerb zu Europa
Entwicklung A	Internationale Kooperation
Entwicklung B	Starker internationaler Wettbewerb und Protektionismus

Tab. 16: Deskriptor D12 (eigene Darstellung)

Die Kommissarin für Informationsgesellschaft und Medien der Europäischen Kommission, Viviane Reding, motiviert in ihrem Grußwort in einem aktuellen Positionspapier des BMWi die Mitgliedsstaaten zu einer stärkeren Zusammenarbeit im Bereich der Forschung für das Internet der Dinge. Sie beschreibt das zukünftig bedeutende wirtschaftliche Potenzial für Europa und unterstreicht die Notwendigkeit, Kontrolle über Erstellung, Verwendung und Aktualisierung der Daten zu behalten,[113] wenn diese nach europäischem Recht behandelt werden sollen. Es wird also deutlich, dass Europa im Wettbewerb zum Rest der Welt steht und die weitere Entwicklung des Internets der Dinge, seiner Infrastruktur und der Betreiber noch offen sind. Das BMWi identifiziert die Vereinigten Staaten von Amerika und Asien als außerordentlich starke Konkurrenten in Forschung und Entwicklung.[114]

Als Gefahr wird vor allem das Betreibermodell von EPCglobal angesehen, wenn es als alternativloses Mittel des Informationsaustausches in Betrieb genommen würde.[115] Die Betreiber könnten bestimmten Teilnehmern Objektnamendienste verweigern oder Warenflüsse der Länder verfolgen.

Alle beschriebenen Einflussfaktoren in Technik, Standardisierung, Wirtschaft, Akzeptanz und gesetzlichen Rahmenbedingungen sind letztlich auch vom internationalen Wettbewerb abhängig. Nach eigenen Überlegungen ist daher nicht so sehr die Frage relevant, welche Nation Technologieführer wird, sondern wie stark die jeweiligen Nationen kooperieren werden.

Entwicklung A beschreibt eine Situation im Jahre 2020, in der zumindest Europa und Amerika stark kooperieren, aber gemeinsam im Wettbewerb zum wirtschaftlich stärker gewordenen Asien stehen. Wie auch in der Entwicklung des heutigen Internets war Amerika in der Entwicklung und Verbreitung des Internets der Dinge führend. Um den wirtschaftlich notwendigen Warenaustausch zwischen Amerika und Europa zu optimieren, ist Europa nach

---

[113] BMWI (2007B), S. 6

[114] BMWI (2007B), S. 11

[115] BMWI (2007B), S. 19

und nach mitgezogen und hat seine Frequenzbereiche denen in Amerika angepasst. In Asien hat sich ein eigenes Internet der Dinge entwickelt, welches jedoch nur begrenzt mit dem europäisch-amerikanischen kompatibel ist. Die wirtschaftliche Kooperation zwischen Europa und Amerika hat die weitere Entwicklung des Internets der Dinge gefördert.

Entwicklung B beschreibt einen stärkeren Wettbewerb zwischen Europa, Amerika und Asien.[116] Der stärkere Wettbewerb hat dazu geführt, dass Europa sich für den Betrieb eines eigenen ONS-Dienstes entschieden hat, um nicht von einer anderen Nation abhängig zu sein. Diese Entscheidung hat die Markteinführung des Internets der Dinge in Europa deutlich verzögert. Im Jahre 2020 ist das neue System, welches kompatibel mit dem EPC-Global-Netzwerk ist, seit einigen Jahren im Betrieb. In Amerika gibt es schon zahlreiche Anwendungen im Endkundenbereich, welche jedoch erst nach und nach in Europa adaptiert werden. Insgesamt hat sich der stärkere Wettbewerb und eine protektionistische Politik hemmend auf die Entwicklung des Internets der Dinge in Europa ausgewirkt.

4.4 Szenario-Zusammenstellung

Die beschriebenen Deskriptoren wurden bewusst jeweils in eine mögliche positive und negative Entwicklungsrichtung hin beschrieben, um eine große Bandbreite an denkbaren Zukunftsszenarien abzubilden. Bei vielen Deskriptoren ließen sich auch zahlreiche weitere Entwicklungsrichtungen beschreiben, worauf jedoch im Hinblick des geplanten Umfangs dieser Arbeit verzichtet wurde. Es sei jedoch erwähnt, dass die Aufführung von nur zwei möglichen Entwicklungsrichtungen keinesfalls bedeutet, dass jeweils nur diese beiden Entwicklungen möglich sind.

Da die Deskriptoren, wie bereits beschrieben, bewusst jeweils ein positives wie auch ein negatives Szenario beschreiben, und auch schon bei ihrer Formulierung auf eine Konsistenz innerhalb der Entwicklungsrichtungen geachtet worden ist, lassen sich nun zwei eindeutige Szenarien im folgenden Kapitel beschreiben. Dabei werden alle Entwicklungsrichtungen mit dem Typ A zu dem Szenario „Das Internet der Dinge ist Wirklichkeit geworden“ zusammengefasst. Alle Entwicklungsrichtungen mit dem Typ B beschreiben das Szenario „Das Internet der Dinge ist eine Nischenanwendung“. Beide Szenarien erfüllen somit die methodischen Anforderungen der Szenariotechnik, auch wenn es sich hier um eine relativ vereinfachte Form handelt.

---

[116] BERTELSMANN-STIFTUNG.DE (2006) am 22.04.2009

5 Szenariobeschreibung für das Internet der Dinge im Jahre 2020

Die Ergebnisse des vorherigen Kapitels werden nun in zwei Szenariobeschreibungen illustriert. Dabei wird versucht, auf möglichst viele Bereiche des täglichen Lebens Bezug zu nehmen, um ein umfassendes Zukunftsbild zu schaffen. FRIEDEWALD[117] stellt im Rahmen einer durchgeführten Szenarioanalyse technischer Entwicklungsprojekte fest, dass besonders häufig die folgenden Bereiche in Zukunftsvisionen beschrieben werden: Privathaushalte, Arbeitsplatz, Gesundheit und Pflege, Shopping und Konsum, Mobilität. Auf alle diese Bereiche sei im Folgenden nun ebenfalls eingegangen. Die Anwendungsbeispiele, die im nächsten Kapitel rechtlich beurteilt werden, sind durch einen *kursiven* Abschnittstitel gekennzeichnet.

5.1 Szenario 1: Schöne neue vernetzte Welt.

Sensoren in Alltagsgegenständen: Harmonische Naturklänge wecken Bernd an diesem Morgen, irgendwann zwischen 6:45 Uhr und 7:15 Uhr. Er hatte zuvor diesen Weck-Zeitraum in seinem neuen Sensorwecker eingestellt, und nun wird er immer in der zum Aufstehen günstigsten Schlafphase geweckt. Kleine Sensoren in seinem Kopfkissen messen die Herzfrequenz und teilen diese seinem Wecker mit.

Intelligente Haustechnik: schön, dass mittlerweile auch die meisten Geräte in seiner Mietwohnung untereinander vernetzt sind – jetzt riecht er bereits den frischen Kaffee in der Küche. Die Tatsache, dass sein Wecker irgendwann einmal mit der Kaffeemaschine sprechen würde, hätte er sich vor nicht allzu langer Zeit nicht einmal vorstellen können. Insgesamt ist jetzt im Jahre 2020 so einiges bequemer geworden: Der Staubsauger findet seinen Weg alleine durch die Wohnung und entscheidet selbst, wann er eine Reinigungstour durchführen muss (dazu misst er den Hausstaubanteil in der Luft). Die Klamotten teilen der Waschmaschine ihr gewünschtes Waschprogramm mit, und die Haustechnik passt sich ihren Bewohnern an. Letzteres gefällt vor allem Franziska gut, der Freundin von Bernd. Sie mag es gerne warm, und daher stellt die intelligente Haustechnik, wenn sie zu Besuch ist, die Temperatur der Heizung automatisch immer etwas höher. Ist niemand im Haus, wird die Heizung heruntergefahren. Dies spart Energie.

Automatische Bestellungen: Doch besonders in einem Bereich wurden in den letzten Jahren, wie Bernd findet, wirklich sinnvolle Fortschritte gemacht: im Dienstleistungsbereich. Die

---

[117] FRIEDEWALD, M. (2007), S. 211-216

Angebote rund um seinen Kühlschrank beschreiben dies besonders gut. Begonnen hatte es damit, dass EasyFood ihm einen neuen Kühlschrank zu einem unglaublich günstigen Preis verkauft hatte. Mit diesem Kühlschrank konnte er später ein ganz spezielles Dienstleistungsangebot in Anspruch nehmen: einen 24-Stunden-Lieferservice von frischen Lebensmitteln, welche durch den Kühlschrank automatisch bestellt werden! Natürlich hatte Bernd im Vorfeld und im Rahmen seines Vertrages seine gewünschte Einkaufsliste konfiguriert. Das Geld, welches ihn der automatische Lieferservice nun monatlich kostet, spart er jetzt durch die Zeitersparnis, da er nicht mehr selbst einkaufen gehen muss. Interessant findet er in diesem Zusammenhang auch, dass ihm kostenlos neue, ihm unbekannte Produkte zum Probieren geliefert werden. Natürlich entsprechen diese Produkte seinem Geschmacksprofil. Gefallen sie ihm, kann er sie in seine regelmäßige Einkaufsliste übernehmen.

Fahrausweise: Nach einem schnellen Frühstück ist es nun aber wirklich Zeit, zur Arbeit zu fahren. Das Firmenauto würde er erst heute Abend nutzen können, und so muss er jetzt den Bus nehmen. Schön, dass man hier keine Fahrkarten mehr kaufen und entwerten muss. Stattdessen hatte Bernd von der Busgesellschaft zuvor einen kleinen Schlüsselanhänger in Form eines Busses erhalten, auf dem seine Kundendaten gespeichert sind. Dieser Schlüsselanhänger regelt nun die Abrechnung der Fahrt. Beim Einstieg wird er dazu einfach kurz vor ein Gerät gehalten bis das ein Signalton zu hören ist. Schon „weis“ der Bus wer gerade wo eingestiegen ist. Indem Bernd auch beim Ausstieg wieder seinen Schlüsselanhänger vor das Gerät hält, wird genau die gefahrene Strecke abgerechnet. Er wird später die Rechnung erhalten. Diese Anwendung hatte er bereits im Jahre 2007 im Skiurlaub kennengelernt.

Mitarbeiterüberwachung: Linda, die hübsche Aushilfe am Empfang von SensoTech – der Firma, in der Bernd arbeitet – begrüßt ihn schon lange nicht mehr. Bereits seit mehreren Jahren wird jetzt der Zugang zum Büro über eine Firmenkarte geregelt, auf der Bernds Mitarbeiterdaten gespeichert sind. Durch diese Firmenkarte wurde auch das lästige Aus- und Einchecken für die Arbeitszeiterfassung überflüssig. Innerhalb der Firma, welche immerhin auf einer Bürofläche von 2.000 qm untergebracht ist, können sich die Kollegen auch dank der Firmenkarte schneller finden. In Echtzeit lässt sich der Aufenthaltsort aller Kollegen im Intranet einsehen. Nach langem Zögern hatte der Betriebsrat dieser Funktion zugestimmt. Klar könnte sein Chef jetzt auch auswerten, mit welchen Kollegen er seine Mittagspause am häufigsten verbringt. In der offen einsehbaren Erläuterung der Hintergrundprozesse ist jedoch

ausdrücklich beschrieben, dass keine sozialen Netzwerke innerhalb der Mitarbeiter analysiert werden.

Es gibt viel zu tun, und so vergeht die Arbeitszeit heute wie im Flug. Ein Ereignis stimmt Bernd aber heute etwas traurig. Peter, ein alter Schulfreund und ebenfalls Mitarbeiter bei SenoTech, wurde gerade nach 15 Jahren Dienstzeit gekündigt. Neben acht weiteren Kollegen arbeitete er in der Produktion und war für das Zusammensetzen einiger Produktreihen verantwortlich. Manchmal war er wirklich etwas zerstreut. Heute jedoch konnten ihm wiederholt eindeutige Fehler in seiner Arbeit nachgewiesen werden. Da alle Produkte über eine eindeutige Seriennummer verfügen, konnte die Geschäftsführung schnell feststellen, wer sie zuletzt bearbeitet hatte.

Nutzungsabhängige Abrechnung: Endlich Feierabend! Es ist doch immer wieder ein tolles Erlebnis, mit dem Firmenwagen zurückzufahren. Natürlich hatte Bernd bereits bei seiner letzten Fahrt das Auto auf seine Bedürfnisse eingestellt. Ein erneutes Einstellen ist nun nicht mehr erforderlich, das Auto hat ihn bereits erkannt und die Einstellungen wieder hergestellt. Auf dem Display in der Mittelkonsole sieht er, dass Sarah, eine Freundin und Kollegin aus der Buchhaltung, gerne mitfahren würde. Sie hatte sich im Internet bei der Mitfahrzentrale angemeldet, und dieses Auto war für diesen Dienst freigeben. Auf der Rückfahrt erzählt sie ihm, wieviel Zeit ihr das neue elektronische Fahrtenbuch des Autos spart, indem es alle Mitfahrer und deren Routen speichert. Versicherungsprämien und Nutzungsgebühren können nun eindeutig und individuell für jeden Nutzer des Firmenautos abgerechnet werden. Oh je, daran hatte er nicht gedacht. Natürlich war er gerne mal einen Umweg gefahren – um auch mal private Sachen zu regeln, wenn er auf dem Weg zu einem Kundentermin war. Nun drohten diese Privatfahrten aufzufallen.

Kundenprofile: Da er aber gerade tatsächlich privat mit dem Auto unterwegs ist, sollte einem Zwischenhalt im Orwell-Einkaufszentrum nichts entgegenstehen. Nachdem er also Sarah zu Hause abgesetzt hat, begibt er sich auf eine kleine Einkaufstour. Immerhin ist wieder Monatsanfang, und damit hat er wieder ein gefülltes Konto. Lange Zeit hatte er den neuen Zusatzangeboten, wie etwa dem digitalen Wegweiser durch das Einkaufszentrum, dem digitalen Einkaufsberater oder den „persönlichen Schnäppchen“-Empfehlungen kritisch gegenübergestanden. Er hatte daher auf eine Kundenkarte verzichtet und sich stets im sogenannten „anonymen Einkaufsbereich“ aufgehalten. In diesem Bereich war er dem Einkaufszentrum als Individuum unbekannt. Das Einkaufszentrum hatte diese Zone für besonders sensible Kunden eingerichtet, um sie nicht durch die neuen technischen Systeme abzuschrecken und letztlich zu verlieren. Doch nach mehreren Jahren positiver Erfahrungen

seiner experimentierfreudigen Bekannten hatte er einer Kundenprofilbildung zugunsten der neuen Angebote zugestimmt. Immerhin hatte er ja die Möglichkeit, sein Kundenprofil im Internet einzusehen, zu verändern und auch zu löschen. Kaum hatte sich sein Handy mit dem Einkaufszentrum verbunden, wurden auch schon die ersten „persönlichen Schnäppchen“ auf seinem Display angezeigt. Die Farbe Pink scheint wieder in Mode gekommen zu sein. Angeblich passt die präsentierte Krawatte besonders gut zu seinem dunkelblauen Hemd, welches er letzten Herbst auch hier gekauft hatte. Ein Klick auf das Produkt zeigt ihm die Position im Einkaufszentrum an. Über Richtungspfeile auf seinem Display wird er auf den Zentimeter genau zum Regal navigiert. Er kauft die Krawatte und bezahlt mit seinem Handy.
Diese Funktion steht jedoch nicht jedem Kunden zur Verfügung. Sie wurde ihm erst kürzlich freigeschaltet nachdem er in eine neue, etwas vornehmere Wohngegend umgezogen war.
Bevormundung: Die neuen Technologien haben aber auch ihre Schattenseiten, wie Bernd bei der Zubereitung des Abendessens bemerken muss. Seine Mikrowelle will einfach nicht sein Fertiggericht aufwärmen. Offenbar ist der eingebaute RFID-Transponder auf der Verpackung seiner Mahlzeit defekt, und nun kann er der Mikrowelle nicht die entsprechende Startanweisung geben. Zum Glück lässt sich die Mikrowelle aber auch noch – wie früher – per Hand bedienen. Ein anderes Beispiel für Schattenseiten der Technologie ist der entstandene Schwarzmarkt für Autozubehör. Sämtliche Autoteile können nur noch als OEM-Ware mit einem vom Hersteller codierten Chip in Betrieb genommen werden. Entspricht die Codierung nicht den Herstellerangaben, werden entweder Warntöne abgespielt oder schlimmer noch, das Fahrzeug lässt sich nicht mehr starten. Auf dem Schwarzmarkt werden daher Ersatzteile mit entsprechenden „gecrackten“ Chips zu einem günstigeren Preis verkauft. Der Markt ist mittlerweile fest in der Hand organisierter Banden.
Heimliches Auslesen: Nach seinem Abendessen erweckt ein Blick von Bernd in die Wohnung von Simone, seiner Nachbarin, welche schräg gegenüber wohnt, seine Aufmerksamkeit: Sie hat einen neuen Fernseher im Wohnzimmer hängen. Es ist ein großes und hauchdünnes Gerät, und Bernd würde gerne mehr darüber wissen. Es ist zwar mittlerweile verboten worden, mittels RFID-Leser fremde Tags auszulesen und technisch kaum noch möglich, doch er hatte im Internet einen Hack gefunden, um die Sicherheitstechniken von Geräten zu umgehen. Kurze Zeit später hat Bernd auch schon die eindeutige Identifikationsnummer des Fernsehers seiner Nachbarin auf dem Display seines Handys mit eingebauter RFID-Leseeinheit. Mittels dieser – üblicherweise verschlüsselten – Nummer kann er nun über einen ONS-Dienst unmittelbar auf die Internetseite dieses Gerätes zugreifen: ein nagelneues Pioneer

Polymerdisplay zum Aufrollen, für 4.000 Euro. Gerade vor zwei Tagen bei Media Markt in Köln gekauft. Wie sie sich so was wohl leisten kann?
Kurze Zeit später klingelt es bei Bernd an der Tür: Simone, seine Nachbarin. Sie sieht ziemlich verärgert aus. Ob sie das heimliche Auslesen durch ein elektronisches Gerät zur Überwachung von unerlaubten Lesezugriffen wohl doch bemerkt hat?

5.2 Szenario 2: Das Ende der Experimentierphase

Bevor im Jahre 2016 in Amerika das EPC-Netzwerk in Betrieb ging, stand für Europa bereits fest, dass es den Betrieb dieses Netzwerkes innerhalb der europäischen Mitgliedsstaaten nicht zulassen würde. Zu groß war mittlerweile der Wettbewerb zwischen Amerika und Europa geworden. Die Wirtschaftskrise von 2008-2012 hatte entschieden dazu beigetragen. Eine wirtschaftliche Abhängigkeit und die Möglichkeit der Verfolgung von Warenströmen durch den potenziellen Wettbewerber durfte nicht riskiert werden. Stattdessen hatte die Europäische Kommission selbst eine technische Infrastruktur geschaffen, welche nahezu identisch mit der amerikanischen ist, sich jedoch in einem wesentlichen Punkt unterscheidet: Die Abfrage von Objektdaten ist nur durch die Übermittlung einer eindeutigen digitalen Signatur für autorisierte Mitglieder möglich. Eine private Nutzung – beispielsweise durch Anwendungen, die Objektdaten mit zusätzlichen Informationen aus Datenbanken verknüpfen – ist daher nicht möglich. Die Vision von Alltagsgegenständen, die ihre eigene Internetseite haben, ist daher nicht zur Wirklichkeit geworden.
Unabhängig von den Diskussionen um die EPC-Infrastruktur hatte zuvor der Metro-Konzern seine Lieferanten verpflichtet, sämtliche Einzelprodukte mit RFID-Transponder zu versehen. Transponder waren deutlich günstiger geworden, da sie sich nun auch mittels Polymertechnologie auf Verpackungen aufdrucken ließen. Für die Lieferanten war der Umstieg nicht sehr aufwändig, da sie zu diesem Zeitpunkt bereits alle eine durch den Metro-Konzern vorgegebene RFID-Infrastruktur zur Optimierung und Automatisierung ihrer Lieferkette eingeführt hatten. Durch die Kennzeichnung von Einzelprodukten sollten in den Läden Personalkosten gespart und eine bessere Verfügbarkeit der Produkte gesichert werden. Abgesehen von einigen Hinweisschildern und sogenannten „Deaktivier-Stationen“ hat sich durch die Einführung der Einzelproduktkennzeichnung mittels RFID-Technologie in den Läden nicht viel verändert. Das Bezahlen an der Kasse geht nun etwas schneller. Die Waren werden auf ein Fließband gelegt und in einem Tunnel gelesen. Statt Kassierer wird nun

Überwachungspersonal beschäftigt, da immer wieder Kunden versuchen, ihre Waren mit Alufolie abzuschirmen.

Viele Unternehmen haben nach Einführung der Einzelkennzeichnung von Produkten mittels RFID-Transponder verstärkt ihre Kundenkarten beworben. So auch der Metro-Konzern, welcher seinen Kunden attraktive Rabatte und Zusatzangebote anbot. Zwei Jahre lang ging alles gut. Dann kam der Skandal: Die Metro hatte für „interne Zwecke“ umfangreiche Kundenprofile angelegt. Neben einer Historie aller gekauften Produkte wurden auch umfassende zusätzliche Informationen erfasst. So wurden die Routen durch die Verkaufsräume, die Einkaufszeiten, die Kaufkraft, die Reaktionen auf Preisänderungen und auch sogar die Beziehung zu anderen Kunden ausgewertet und mit den Angaben auf der Kundenkarte verknüpft.

Datenverarbeitung im Ausland: aufgrund eines interessanten Bonussystems hatten viele Kunden einer „Verarbeitung von Daten mit Personenbezug für interne Zwecke“ zugestimmt. Die Verarbeitung erfolgte dabei in Mexiko – für die Metro war die Gesetzeslage hier etwas günstiger.

Inspiriert von den kriminell verkauften Bankdaten einiger Privatanleger an die Staatsanwaltschaft im Jahre 2008, hatte ein Mitarbeiter des Metro-Konzerns in den Kundenprofilen das große Geld gewittert und diese an meistbietende Unternehmen verkauft. Das eigentliche Ausmaß dieses Datenskandals wurde uns erst nach und nach bewusst: Lebens- und Autoversicherungen zahlreicher Bürger wurden gravierend teurer, einige wurden sogar gekündigt. Als Begründung wurde eine „unverantwortliche Lebensweise durch übermäßigen Alkohohl-Konsum“ angegeben. Schlimm war auch die ganze Werbung, welche Infolge dieses Datenskandals als personalisierter „Spam“ auf uns zukam.

Die Regierung hatte stets in den bestehenden Datenschutzgesetzen einen ausreichenden Schutz für die Bürger gesehen. Auch wir fühlten uns durch die Gesetze ausreichend geschützt. Erst nach Bekanntwerden des Skandals wurden neue Gesetze erlassen, und unsere Einstellung zur Bekanntgabe persönlicher Angaben hat sich seitdem auch stark verändert. Wir sind insgesamt vorsichtiger geworden und machen nicht mehr alles mit.

Gesundheitsdaten: Ich glaube, jetzt – im Jahre 2020 – haben wir die Experimentierphase hinter uns gebracht und erkennen nun besser, in welchen Bereichen die neuen Technologien sinnvoll einzusetzen sind. So beispielsweise im Gesundheitsbereich. Unsere Oma Anna kann aufgrund eines Schlaganfalls nicht mehr gut laufen. Sie wird daher in einer Pflegepension betreut. Natürlich gehen wir sie regelmäßig besuchen, aber dank der neuen Technologien können wir ihren Gesundheitszustand mittels einer speziellen VPN-Verbindung auch von zu

Hause aus überwachen. Dabei erhalten wir die selben Informationen, die auch die Ärzte in der Pflegepension einsehen können. Weltweit hat sich auch die Qualität der Medikamente verbessert, da Plagiate von wichtigen Medikamenten eindeutig identifiziert werden können.
So, jetzt habe ich Ihnen aber schon eine ganze Menge erzählt. Es wird für mich nun Zeit, zur Arbeit zu gehen. Ich arbeite übrigens in einem Unternehmen, welches sich auf die Auto-Identifikation von Objekten spezialisiert hat. Momentan gibt es bei uns viel zu tun. Greenpeace hat der Europäischen Kommission nachgewiesen, dass sich die Qualität von Rohstoffen aus Mehrwegverpackungen in den letzten Jahren signifikant verschlechtert hat. Jetzt gilt es für uns, neue Verfahren für das Recycling von RFID-Transponder zu entwickeln. Sonst droht die Kommission, die Kennzeichnung von Mehrwegverpackungen mittels RFID-Technologie zu untersagen. Einige Handelsketten und Bioläden haben sich bereits wieder von der RFID-Technologie distanziert und setzen neuerdings auf die Lasertechnologie. Zwar ist hier ein Sichtkontakt zum Lesegerät erforderlich, doch die Kunden vertrauen dieser Technologie deutlich mehr, da ein heimliches Auslesen nicht möglich ist. Zum Glück hat unser Unternehmen das Potenzial der Lasertechnologie frühzeitig erkannt und erforscht in diesem Bereich aktuell auch neue Anwendungsmöglichkeiten.

6 Rechtliche Bewertung der Szenarien

Stellen die skizzierten Anwendungen in den Szenarien eine Gefahr der permanenten Überwachung der Bevölkerung durch Unternehmen, Arbeitgeber und neugierige Nachbarn dar, oder bietet die deutsche und europäische Rechtsprechung einen ausreichenden Schutz gegen die Möglichkeiten dieser Überwachung? Das folgende Kapitel versucht, Antworten auf diese Frage zu geben. Da die rechtliche Beurteilung immer von dem jeweiligen Umfeld und der Rolle des „Beobachteten“ abhänget, werden zunächst die relevanten Gesetze und deren Anwendungsrahmen beschrieben. Der Fokus liegt hier besonders auf dem Bundesdatenschutzgesetz, da es für alle Anwendungsbeispiele relevant ist. Im Anschluss werden elf Anwendungsbeispiele der beschriebenen Szenarien auf Grundlage der aktuellen Rechtsprechung beurteilt. Das Kapitel endet mit einer Darstellung der Grenzen heutiger Datenschutzgesetze und mit einem Ausblick auf deren möglicher Modernisierung.

6.1 Anwendbarer Rechtsrahmen

Für die rechtliche Bewertung der Anwendungsbeispiele spielen die unterstellten Rahmenbedingungen in den Szenarien eine bedeutende Rolle. Kleine Details können hier das Ergebnis der Bewertung entscheidend beeinflussen. Die TAUCIS-Studie bestätigt in diesem

Zusammenhang, dass eine rechtliche Bewertung nur auf einen konkreten Anwendungsfall bezogen durchgeführt werden kann. Hierbei spielen das Umfeld, die Rollen der beteiligten Personen sowie deren Informations- und Einflussmöglichkeiten eine bedeutende Rolle.[118] Je nach Anwendungsumfeld können neben dem Bundesdatenschutzgesetzt (BDSG) – welches später noch im Detail erläutert wird – auch andere Gesetze eine Rolle spielen. Nachfolgend sei der Rechtsrahmen für die Umfelder Wohnung, Arbeit, Konsum und Gesundheit zusammenfassend dargestellt.

Umfeld Wohnung: Im Umfeld der privaten Wohnung sind zahlreiche Anwendungen allgegenwärtiger Datenverarbeitung denkbar. Wie im Anwendungsbeispiel beschrieben, können solche Systeme zu mehr Komfort der Bewohner beitragen oder auch schlichte Zugangs- und Sicherheitssysteme darstellen. Für eine rechtliche Bewertung solcher Anwendungen ist daher zunächst die Rolle des Betroffenen zu klären, der in einer Privatwohnung Mieter, Eigentümer, Arbeitnehmer, Verbraucher oder Besucher sein kann. Neben dem BDSG finden je nach Rolle des Betroffenen eine Vielzahl weiterer Gesetze Anwendung: das Arbeitsrecht, wenn etwa Reinigungspersonal beschäftigt wird; das Verbraucherrecht, wenn Einkäufe getätigt werden; das Telekommunikations- und Medienrecht bei der Nutzung von Kommunikationsgeräten sowie die Grundsätze des Persönlichkeitsschutzes, wenn etwa Gäste in den Einflussbereich der datenerhebenden Anwendungen gelangen.

Umfeld Arbeit: Am Arbeitsplatz können Anwendungen allgegenwärtiger Datenverarbeitung zu Bewegungsprofilen und zu einer Überwachung der Arbeitsleistung von Arbeitnehmern eingesetzt werden, welche – wie im Anwendungsszenario beschrieben – auch das individuelle Fehlverhalten einzelner Mitarbeiter nachweisen können. Solche Systeme werden in der Regel vom Arbeitgeber im Rahmen seines Direktionsrechtes vorgegeben, und Beschäftigte können auf deren Gestaltung nur begrenzt Einfluss nehmen.[119] Die Verarbeitung personenbezogener Daten ist aber grundsätzlich nur dann zulässig, wenn ein Erlaubnistatbestand gegeben ist, der sich aus einer Betriebsvereinbarung (beispielsweise Arbeits- oder Tarifvertrag) ergeben kann. Ist ein Betriebsrat vorhanden, so ist eine Erhebung von personenbezogenen Daten im Rahmen einer Betriebsvereinbarung grundsätzlich auch mitbestimmungspflichtig. Zusammenfassend stellen neben dem BDSG das Arbeitsrecht und Dienstvereinbarungen die Grundlage für eine rechtliche Bewertung allgegenwärtiger Datenverarbeitung im Arbeitsumfeld.

---

[118] TAUCIS (2006), S. 101

[119] TAUCIS (2006), S. 101

Umfeld Konsum / Dienstleistung: Im Konsumumfeld können durch RFID-gekennzeichnete Produkte Kundenprofile erstellt werden. Diese müssen anfangs nichts zwangsläufig auch einen direkten Personenbezug enthalten. Werden aber später solche „Pseudoprofile“ an der Kasse mit persönlichen Angaben – etwa von einer Bank- oder Kundenkarte kombiniert – kann eine erhebliche Gefahr für den Verbraucher entstehen. Hier greift neben dem BDSG auch der Verbraucherschutz ein. Dem Leitbild des „mündigen Verbrauchers“ entsprechend,[120] stellt er einen fairen Leistungsaustausch beider Seiten durch die Herstellung oder den Erhalt eines Verhandlungsgleichgewichts sicher. Überwiegen also die Vorteile für den Anbieter, kann das Verbraucherschutzrecht angewendet werden.

Werden zur Erfüllung von Dienstleistungen personenbezogene Daten erhoben oder verarbeitet, muss gemäß des BDSG grundsätzlich eine Einwilligung des Betroffenen vorliegen. Im Rahmen einer freien Vertragsgestaltung kann diese jedoch in einem vorher abgeschlossen Dienstleistungsvertrag erteilt worden sein. Wichtig ist an dieser Stelle die Freiwilligkeit der Einwilligung.

Umfeld Gesundheit: Im Gesundheitswesen sind zahlreiche Anwendungen allgegenwärtiger Datenverarbeitung denkbar. Diese können neben der automatisierten Erfüllung von Routineaufgaben auch kritische Aufgaben übernehmen, etwa wenn eine Körperfunktion eines Patienten überwacht oder aufrechterhalten wird. Durch den Einsatz solcher Anwendungen wird eine Vielzahl sehr sensibler personenbezogener Daten in Hintergrundsystemen verarbeitet. Der rechtliche Rahmen ergibt sich aus §3 Absatz 9 BDSG, der diese Daten als besondere Daten definiert, die besonderen Berufs- oder Amtsgeheimnissen unterliegen.

6.2 Das Bundesdatenschutzgesetz

Das BDSG schützt den Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.[121] Damit sichert das BDSG das Recht auf informationelle Selbstbestimmung, welches die Bürger grundsätzlich selbst darüber entscheiden lässt, in welchem Umfang persönliche Daten erhoben oder verwendet werden. Das Recht auf informationelle Selbstbestimmung wurde durch das sogenannte Volkszählurteil des Bundesverfassungsgerichtes (BVerfG) vom 15.12.1983 als Grundrecht anerkannt. [122]

---

[120] TAUCIS (2006), S. 123, zitiert BORCHERT, G. (1994), S. 1

[121] §1 Absatz 1 BDSG

[122] BVerfGE 65, 1

Anwendungsbereich: Das BDSG findet gemäß §1 Absatz 2 BDSG Anwendung bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Diese werden nach §3 Absatz 1 BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (nachfolgend „Betroffener“) definiert. Die Datenschutzregeln des BDSG richten sich grundsätzlich an drei unterschiedliche Adressaten (nachfolgend „Verantwortliche Stelle“): öffentliche Stellen des Bundes, öffentliche Stellen der Länder und nicht-öffentliche Stellen. Die Anwendbarkeit des Datenschutzrechts hängt auch maßgeblich davon ab, ob die Daten verarbeitende Stelle ihren Sitz innerhalb oder außerhalb des Europäischen Wirtschaftsraumes (EWR) hat. Werden Daten außerhalb des EWR verarbeitet, gilt das sogenannte Territorialitätsprinzip, wonach es für die Anwendbarkeit des Gesetzes auf den Ort der Datenerhebung ankommt.

Das BDSG basiert im Wesentlichen auf datenschutzrechtlichen Grundprinzipien, welche nachfolgend beschriebenen werden:

Datenverarbeitungsverbot mit Erlaubnisvorbehalt: Nach §4 Absatz 1 BDSG herrscht ein generelles Datenverarbeitungsverbot mit Erlaubnisvorbehalt. Nur wenn der Betroffene eingewilligt hat oder eine gesetzliche Erlaubnisvorschrift greift, können personenbezogene Daten erhoben und verarbeitet werden.

Grundsatz der Direkterhebung: Gemäß §4 Absatz 2 BDSG setzt eine rechtmäßige Datenerhebung grundsätzlich voraus, dass die personenbezogenen Daten bei den Betroffenen selbst und mit ihrer Kenntnis erhoben werden. Nur in festgelegten Ausnahmefällen dürfen Daten auch ohne Mitwirkung des Betroffenen erhoben werden.

Zweckbindungsgrundsatz: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gemäß §14 Absatz 1 BDSG nur für festgelegte, eindeutige und rechtmäßige Zwecke zulässig. Diese Zwecke müssen bei der ersten Datenerhebung bestimmt sein und können gemäß §39 BDSG einer besonderen Zweckbindung mit strengeren Vorschriften unterliegen, wenn sie bestimmte Berufs- oder Amtsgeheimnisse betreffen. Für Ärzte gelten beispielsweise spezielle Berufsgeheimnisse.

Erforderlichkeit: Anknüpfend an den Zweckbindungsgrundsatz dürfen gemäß §28 Absatz 1 BDSG nur solche Daten erhoben und verarbeitet werden, die zur Erfüllung des jeweiligen Zweckes mindestens erforderlich sind. Es ist also grundsätzlich zu prüfen, ob die Erhebung und Verarbeitung von Daten erforderlich ist, oder ob es eine zumutbare Alternative zur Erfüllung des Zweckes gibt.

Datenvermeidung und Datensparsamkeit: Bereits vor der Gestaltung und Auswahl technischer Systeme haben Daten verarbeitende Stellen, gemäß §3a BDSG, Datenvermeidung

und Datensparsamkeit zu berücksichtigen. Somit soll dem Datenschutz bereits im Vorfeld der Erhebung Rechnung getragen werden. Weiterhin ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Transparenz: Das Transparenzgebot beschreibt sowohl Pflichten der verantwortlichen Stelle gegenüber den Betroffenen als auch organisatorische. Zu den Transparenzpflichten gegenüber den Betroffenen zählen Unterrichtungs-, Hinweis- und Aufklärungspflichten bei der Datenerhebung. Der Betroffene soll damit in die Lage versetzt werden, selbst zu entscheiden, ob er seine Daten preisgeben möchte oder nicht. Außerdem soll gemäß §4 Absatz 3 BDSG sichergestellt werden, dass der Betroffene über Art, Umfang und Zweck der ihn betreffenden Datenverarbeitung Kenntnis hat und gegebenenfalls diese Daten berichtigen oder löschen kann. Zu den organisatorischen Transparenzpflichten zählt, dass gemäß §4g Absatz 2 BDSG bei automatisierten Verfahren ein sogenanntes Verfahrensverzeichnis zu erstellen ist, welches dem betrieblichen Datenschutzbeauftragen zur Kontrolle und gegebenenfalls Veröffentlichung zu übergeben ist.

6.3 Datenschutz auf europäischer Ebene

Auf europäischer Ebene ist der Datenschutz sowohl im EU-Vertrag selbst als auch in weiteren Verordnungen und Richtlinien für die Mitgliedsstaaten verankert. Im Vertrag über die Europäische Union (EUV) sind nach Artikel 6 alle EG-Institutionen auch zur Beachtung des Grundrechtes auf Datenschutz verpflichtet. Die Rechtsprechung des Europäischen Gerichtshofes verweist hier insbesondere auf die Europäische Menschenrechtskonvention (EMRK), welche in Artikel 8 das Recht auf Privatsphäre und Datenschutz gewährleistet. Die 1995 verabschiedete Richtlinie 95/46/EG stellt einen weiteren, international wirkenden Schutz der Privatsphäre dar. Sie regelt den freien Datenverkehr im europäischen Binnenmarkt und verbietet den Transfer von personenbezogenen Informationen in „nicht sichere Drittländer“. Die Richtlinie legt allgemeine Grundsätze für die Qualität und die Zulässigkeit der Verarbeitung von personenbezogenen Daten fest. Alle Mitgliedstaaten der Union werden zur Einhaltung eines vorgeschriebenen Mindestschutzes personenbezogener Daten sowie zur Angleichung ihrer nationalen Gesetzgebung – der Richtlinie entsprechend – verpflichtet. In Deutschland erfolgte diese Angleichung im Rahmen der Novellierung des BDSG vom 23.5.2001, welche die Anforderungen der EG-Richtlinie in nationales Recht umgesetzt hat. In der nun folgenden Bewertung der Szenarien kann also davon ausgegangen werden, dass aufgrund der Richtlinie 95/46/EG in anderen europäischen Ländern weitgehend die gleichen rechtlichen Rahmenbedingungen herrschen wie auch in Deutschland.

6.4 Rechtliche Bewertung der Szenarien

In der nun folgenden rechtlichen Bewertung der Szenarien werden die relevanten Rahmenbedingungen der Anwendungsbeispiele zunächst kurz zusammengefasst und die Rollen der beteiligten Personen definiert. Anschließend wird die rechtliche Zulässigkeit des Falles gemäß relevanter Gesetze überprüft, und es wird versucht, mögliche rechtliche Schwachstellen zu skizzieren.

Sensoren in Alltagsgegenständen: Sensoren in Alltagsgegenständen erfassen im Beispiel Daten aus ihrer Umgebung um den Komfort für den Betroffenen zu erhöhen. Die Erfassung und Verarbeitung erfolgt in einer privaten Umgebung. Der Betroffene ist hier in der Rolle des Nutzers, welcher die Technologien bewusst anwendet und selbst konfigurieren kann. Fraglich ist, ob personenbezogene oder personenbeziehbare Daten erhoben und durch Dritte verarbeitet werden. Dies ist hier nicht der Fall, da die Verarbeitung der Daten – in diesem Falle beispielsweise der Erfassung der jeweiligen Schlafphase – durch die Endgeräte in der privaten Umgebung des Betroffenen selbst verarbeitet werden und Dritten nicht zugänglich sind. Das skizzierte Anwendungsbeispiel ist daher datenschutzrechtlich unbedenklich. Dennoch geht von diesem Beispiel eine Gefahr der Überwachung aus: Es könnten Log-Daten gespeichert werden, welche beispielsweise von einer neugierigen Freundin eingesehen werden könnten. Diese könnten Unregelmäßigkeiten in den Schlafphasen nachweisen, ein Personenbezug wäre in diesem Falle einfach herzustellen. Auch Nachbarn könnten die übersandten Daten der Sensoren unerlaubt empfangen und damit Rückschlüsse – zumindest, ob jemand im Bett liegt oder nicht – ziehen. Hier spielt die Technikgestaltung solcher Anwendungen also auch eine bedeutende Rolle. Von den Herstellern sollten Verschlüsselungsverfahren für die Datenübertragung vorgesehen werden.

Intelligente Haustechnik: Ähnlich zur vorherigen Situation werden in diesem Beispiel Daten aus dem Umfeld der privaten Wohnung erhoben. Welche Daten dies genau sind wird nicht beschrieben. Jedoch wird durch die erhobenen Daten ein Personenbezug hergestellt, da beschrieben wird, dass das System für die jeweiligen erkannten Personen entsprechende Voreinstellungen abrufen kann. Die Rolle des Betroffenen wird hier als Mieter beschrieben. Wie und von wem die erhobenen Daten verarbeitet werden, wird nicht beschrieben, auch nicht, ob die Daten an den Vermieter oder den Gasanbieter übertragen werden. Aufgrund des offensichtlichen Personenbezuges finden die Grundsätze des BDSG Anwendung. Der Betroffene muss in diesem Falle von der verarbeitenden Stelle – in diesem Falle dem Betreiber des Systems – über das Vorhandensein und die Art und Weise der

Datenverarbeitung informiert worden sein. Ein solches System ist also in den Mietvertrag ausdrücklich einzubeziehen. Durch Annahme des Mietvertrages erteilt der Mieter dem Vermieter die Einwilligung zur Datenerhebung. In diesem Falle stehen ihm jederzeit Auskunfts- und Korrekturrechte zu. Der Vermieter könnte zwar das Verhalten des Mieters heimlich überwachen, jedoch sind dessen Rechte durch das BDSG weitestgehend gesichert, und er kann die Löschung seiner nicht mehr erforderlichen Daten verlangen. Jedoch ist der Vermieter nicht dafür verantwortlich, was der Mieter selbst mit den erhobenen Daten – beispielsweise denen seiner Gäste – macht. Für letztere wird es in der Regel schwer erkennbar sein, dass personenbezogene Daten erhoben und verarbeitet werden. Eine rechtliche Durchsetzung der Ansprüche von Betroffenen wird sich hier als schwierig erweisen.

Automatische Bestellungen: Im Anwendungsbeispiel tätigt der Kühlschrank des Betroffenen selbst Bestellungen. Das Umfeld ist hier die Privatwohnung des Betroffenen, der in diesem Falle die Rolle des privaten Verbrauchers einnimmt. Fraglich ist, ob personenbezogene Daten übermittelt werden. Dies ist hier der Fall, da vom Kühlschrank Bestellungen an den Dienstleister übermittelt werden. Dort werden diese Bestellungen offenbar mit einem Kundenkonto und den jeweiligen Vertragsbedingungen abgeglichen, um eine Lieferung von neuer Ware zu veranlassen. Der Dienstleister ist demnach in der Lage, ein Profil des Kunden zu erstellen. Das BDSG findet in diesem Falle Anwendung. Voraussetzung für eine rechtmäßige Abwicklung ist die Einwilligung des Betroffenen und dessen vorherige Unterrichtung über den Zweck und die Art der Datenverarbeitung. Die Einwilligung ist im Beispiel durch einen abgeschlossenen Dienstleistungsvertrag erfolgt. Damit stehen dem Betroffen auch hier wieder entsprechende Auskunfts- und Kontrollmöglichkeiten zu. Eine entsprechende Protokollierung der übermittelten Daten, welche durch den Betroffen einsehbar ist, könnte dies gewährleisten. Der Dienstleister hat ferner dafür zu sorgen, dass nur die zum Zweck der Vertragserfüllung notwendigen Daten erhoben werden. Das beschriebene Anwendungsbeispiel ist daher in dieser Form zulässig. Der Schutz des Betroffenen ist durch das BDSG gewährleistet.

Fahrausweise: Elektronische Fahrkartensysteme sind bereits seit einiger Zeit im realen Einsatz. Auf einer vom Anbieter ausgegebenen Karte sind die Daten des Besitzers gespeichert. Diese werden im Bus ausgelesen und durch ein Hintergrundsystem des Anbieters verarbeitet. Durch die Erhebung solcher personenbezogener Daten könnte der Anbieter Bewegungsprofile des Betroffenen erstellen und diese sogar anderen zugänglich machen. Aufgrund der Verarbeitung personenbezogener Daten findet jedoch das BDSG Anwendung. Demnach muss der Anbieter den Betroffenen vor Vertragsabschluss über die Verarbeitung

und Speicherung seiner persönlichen Daten unterrichten, und dieser muss dem freiwillig zustimmen. Der Anbieter hat ferner gemäß §9 BDSG technische und organisatorische Maßnahmen zu Schutzzwecken so zu berücksichtigen, dass Dritte keinen Zugriff auf diese Daten haben. Dies wird in der Praxis durch kryptografische Verfahren gelöst, indem nur die Lesegeräte des Betreibers die Karten der Betroffenen lesen können. Dem Grundsatz der Transparenz nach muss der Anbieter dem Betroffenen auch signalisieren, wann ein Lesevorgang erfolgt. Dies kann beispielsweise durch ein optisches oder akustisches Signal erfolgen. Durch einen Kundenzugang im Internet könnte ein Betroffener auch seine gespeicherten Daten einsehen und bei Bedarf löschen.

Mitarbeiterüberwachung: Im Arbeitsumfeld sind durch den Einsatz allgegenwärtiger Datenverarbeitung zahlreiche Überwachungsmöglichkeiten der Arbeitnehmer denkbar. Neben der Erfassung von Arbeitszeiten können Aufenthaltsorte, Routen, soziale Netzwerke und Verantwortlichkeiten einzelner Mitarbeiter erfasst und ausgewertet werden. Im beschriebenen Anwendungsbeispiel werden mittels einer Mitarbeiterkarte Zugänge ermöglicht, Leistungen von Einzelpersonen erfasst und eine Ortsbestimmung in Echtzeit betrieben. Verantwortliche Stelle ist hier der Arbeitgeber, Betroffener ist hier der Arbeitnehmer. Da personenbezogene Daten verarbeitet werden, greifen hier die Bedingungen des BDSG. Demnach hat für den rechtsmäßigen Betrieb solcher Anwendungen zunächst eine Einwilligung der Betroffenen zu erfolgen. Eine entsprechende Rechtsgrundlage können hier Dienstvereinbarungen darstellen, die der Arbeitnehmer akzeptieren muss, wenn er das Beschäftigungsverhältnis erhalten möchte. Eine Freiwilligkeit ist hier also eher fragwürdig. Aber es besteht eine Mitbestimmungspflicht, wenn ein Betriebsrat vorhanden ist.[123] In jedem Falle sind die Systeme so zu gestalten, dass technische und organisatorische Maßnahmen das Missbrauchspotential reduzieren. Eine Lösung gegen ein verdecktes Auslesen könnte beispielsweise eine abschirmende Hülle für die Mitarbeiterkarte sein, die auch eine Mitwirkung des Arbeitnehmers bei der Datenerhebung erforderlich macht. Zusammenfassend ist das dargestellte Anwendungsbeispiel damit zulässig. Eine umfassende Beobachtung der Mitarbeiter ist mit Hilfe der neuen technologischen Möglichkeiten anwendbar, wenn die Mitarbeiter über das Vorhandensein und die Funktion der Systeme informiert worden sind und durch ihren Arbeitsvertrag der Erhebung und Verarbeitung ihrer persönlichen Daten zugestimmt haben.

---

[123] §87 Absatz 1 Nr. 6 BetrVG

Nutzungsabhängige Abrechnung: Im dargestellten Anwendungsfall werden personenbezogene Daten über die Fahrweise des Betroffenen an seine Autoversicherung übersandt, welche dafür eine nutzungsabhängige Abrechnung ihrer Versicherungsleistung anbietet. Das BDSG findet hier Anwendung. Wie auch in den anderen Fällen hat hier zunächst eine Einwilligung des Betroffenen zu erfolgen. Das Versicherungsunternehmen muss den Interessenten vorab über die genaue Art der Datenerhebung unterrichten und ihm alle bereits erwähnten Kontroll-, Einsichts- und Korrekturmöglichkeiten bieten. Wenn der Interessent diesen Versicherungsvertrag annimmt, ist eine solche Anwendung im Rahmen einer freien Vertragsgestaltung grundsätzlich zulässig.

Kundenprofile: Kunden sind oft bereit, für die Einräumung kleiner Rabatte persönliche Daten preiszugeben.[124] Nach diesem Prinzip werden bereits seit Jahren Kundenkarten, welche den Unternehmen Auskunft über die Konsumgewohnheiten ihrer Kunden geben, mit Rabatten verknüpft. Kundenkarten sind nicht nur in Deutschland sehr beliebt. Im Anwendungsbeispiel befindet sich der Betroffene in der Rolle des Verbrauchers. Auf seiner freiwillig bezogenen Kundenkarte sind seine persönlichen Angaben gespeichert. Wie auch in den bereits beschriebenen Fällen kann er der verarbeitenden Stelle, hier also dem Unternehmen, eine Einwilligung zur Erhebung und Verarbeitung seiner persönlichen Daten zum Zwecke eines Bonusprogramms erteilt haben. Fraglich ist jedoch, welche Daten zur Erfüllung dieses Zweckes erhoben werden müssen. Gemäß dem Prinzip der Erforderlichkeit dürfen nur die Daten erhoben werden, die zur Erfüllung des jeweiligen Zweckes erforderlich sind. Es ist sehr fraglich, ob das Erheben der individuellen Einkaufsgewohnheiten von Verbrauchern erforderlich ist, um ein Bonusprogramm zu rechtfertigen, oder ob vielmehr durch das Sammeln dieser Daten ein alternativer Zweck beabsichtigt wird. Dieser alternative Zweck, beispielsweise der Abschluss neuer Verträge oder die gezielte individuelle Produktwerbung, würden eine Zweckänderung darstellen, welche einer eigenen Rechtsgrundlage und Zustimmung bedürfen würde.[125] Auch wären in jedem Falle wieder die gesetzlichen Auskunfts- und Korrekturmöglichkeiten für Betroffene zu berücksichtigen. Kundenprofile können im Extremfall auch zu Preisdiskriminierungen verwendet werden. Da jedoch in diesem Falle ein erheblicher Wissensüberschuss des Anbieters ausgenutzt würde, könnte hier das Verbraucherschutzrecht Anwendung finden, welches einen Erhalt des Verhandlungsgleichgewichtes anstrebt.[126] Im Anwendungsbeispiel hat der Betroffene die freie

---

[124] LANGHEINRICH, M. (2004), S.2

[125] TAUCIS (2006), S. 117

[126] TAUCIS (2006), S. 123

Einwilligung zur Verarbeitung seiner persönlichen Daten gegeben, um entsprechende Zusatzleistungen in Anspruch zu nehmen. Wenn diese als Zweck der Datenerhebung angegeben wurden, eine entsprechende Erhebung einzelner Angaben für deren Erfüllung erforderlich ist und die Regelungen des BDSG beachtet werden, ist das Beispiel hier zulässig.

Bevormundung: Die technologisch bedingte Bevormundung von Verbrauchern stellt zwar kein Datenschutzproblem dar, kann sich aber künftig als ein wirtschaftliches Problem herausstellen. Im Anwendungsbeispiel verwährt die Mikrowelle das Aufwärmen eines Fertiggerichtes. Dies könnte der Fall werden, wenn Alltagsprodukte mit RFID-Technologie gekennzeichnet werden. Die Mikrowelle könnte dann beispielsweise nur das Erwärmen einer bestimmten – teureren – Marke erlauben. Ein reales Beispiel sind Nachfüllpatronen von Druckern, welche zum Schutze von günstigen Plagiaten bereits heute mit RFID-Technologie ausgestattet werden.[127] Zur rechtlichen Beurteilung können auch hier die Prinzipien des Verbraucherschutzes angewandt werden. Es ist im Einzelfall zu prüfen, ob der Endverbraucher durch diese Art der Bevormundung einen Nachteil hat.

Heimliches Auslesen: Wenn zukünftig Produkte des alltäglichen Lebens mit RFID-Transpondern versehen werden, welche – zumindest dem EPC-Standard gemäß – auch unverschlüsselt ausgelesen werden können, besteht eine Gefahr des heimlichen Auslesens von mitgeführten Produkten durch Dritte, was den Inhalt einer Tasche oder einer Wohnung transparent machen könnte. Die Prinzipien des BDSG sind hier schwierig anzuwenden, da hier keine für das System „verantwortliche Stelle“ zur Verantwortung gezogen werden kann. Jedoch ist die Vertraulichkeit der Kommunikation innerhalb von RFID-Systemen auch durch das Fernmeldegeheimnis (TKG) geschützt. Dieses verbietet in §89 TKG ein generelles beabsichtigtes Auslesen von Transpondern. Die Vertraulichkeit wird zusätzlich durch die Straftatbestände der §§148 Absatz 1 Nr. 1 TKG und 202a StGB abgesichert.[128] Zusammenfassend ist das heimliche Auslesen also verboten, aber grundsätzlich in der Praxis möglich. Da das Auslesen unbemerkt erfolgt, ist es fraglich, ob der Betroffene seine Rechte sinnvoll durchsetzen kann. In der Praxis besteht hier also ein reales Überwachungspotenzial.

Datenverarbeitung im Ausland: Die Anwendbarkeit des BDSG ist für eine Erhebung und Verarbeitung von personenbezogenen Daten gegeben. Für die Anwendbarkeit kommt es nach dem sogenannten Territorialitätsprinzip auch auf den Sitz der Daten verarbeitenden Stelle an. Innerhalb von Europa schützt die EG-Datenschutzrichtlinie die Betroffenen. Eine

---

[127] PRODUKTION (2008)

[128] INFORMATIONSFORUM RFID (2008), S. 56

Übermittlung von personenbezogenen Daten ist gemäß Artikel 25 der Richtlinie 95/46/EG nur in Drittländer mit einem angemessenen Schutzniveau zulässig. Ein Problem entsteht jedoch dann, wenn die übermittelten Daten den Personenbezug erst im Drittland – etwa über ein Data Mining – erhalten. In diesem Falle unterliegen sie nicht mehr dem Schutz deutscher und europäischer Rechtsprechung.[129] Das aufgezeigte Anwendungsbeispiel stellt daher ein reales Risiko dar.

Gesundheitsdaten: Der Zugriff auf Gesundheitsdaten von Betroffenen ist für Ärzte, Verwandte, Arbeitgeber, staatliche Stellen und Krankenversicherungen sehr interessant. Für Betroffene kann diese Kenntnis große soziale und wirtschaftliche Konsequenzen haben. Manchmal sind Betroffene auch nicht mehr selbst in der Lage, eine eigene Einwilligung zur Verarbeitung ihrer personenbezogenen Daten zu geben. Aus diesem Grunde unterliegen Gesundheitsdaten besonderen Schutzmaßnahmen, welche in §28 Absatz 6 bis 9 BDSG definiert werden. Demnach ist eine Erbebung ohne Einwilligung unter anderem möglich, wenn sie dem Schutze lebenswichtiger Interessen des Betroffenen dient, oder zum Zwecke der Gesundheitsvorsorge oder für die Behandlung erforderlich ist. In jedem Falle ist die Erhebung und Verarbeitung von Gesundheitsdaten gemäß §28 Absatz 7 BDSG nur durch Personen zulässig, die einer entsprechenden Geheimhaltungspflicht unterliegen. Gemäß §28 Absatz 8 BDSG ist eine Übermittlung oder Nutzung dieser besonderen personenbezogenen Daten für die im Beispiel aufgezeigte Anwendung also nicht zulässig.

6.5 Grenzen des Datenschutzes

Die in den Anwendungsbeispielen skizzierten Fälle können als einfach strukturiert bezeichnet werden: In allen Fällen sind die Rollen der Betroffenen relativ klar definierbar. Auch sind der Zweck der Datenerhebung und die Daten verarbeitende Stelle den Beteiligten bekannt. Die Betroffenen sind aufgeklärt worden und können entsprechende Kontrollrechte geltend machen. In diesen Fällen stellt das BDSG, wie dargestellt, in den meisten Fällen einen ausreichenden Schutz dar. In der Realität werden sich die Anwendungsmöglichkeiten allgegenwärtiger Datenverarbeitung aber weitaus komplexer darstellen. Nach ROSSNAGEL[130] werden sich vielfach komplexere Strukturen ergeben, welche er wie folgt beschreibt: Es sind viele Beteiligte vorhanden, deren Rollen ständig wechseln; die Grenzen zwischen privater und geschäftlicher Nutzung werden sich stärker vermischen, durch die Datenerhebung werden mehrere Zwecke verfolgt, und die Datenerhebung wird vielfach durch die Technik selbst

[129] ROSSNAGEL, A. (2007B), S. 128

[130] ROSSNAGEL, A. (2007B), S. 128

erfolgten, ohne dass ein Betroffener es überhaupt bemerkt. In der TAUCIS-Studie wird diese Situation auch als technikbedingter Kontrollverlust beschrieben.[131] Alle Prinzipien des BDSG – wie etwa das der Einwilligung, der Zweckbindung, der Transparenz, der Datenvermeidung und der Kontrolle – stehen für ROSSNAGEL im Widerspruch zu den Zielen, die mit Hilfe allgegenwärtiger Datenverarbeitung verfolgt werden.[132] Auf diese neuen Verhältnisse seien die Grundsätze des datenschutzrechtlichen Schutzprogramms kaum anwendbar.

6.6 Mögliche Modernisierung des Datenschutzgesetzes

Wie könnte das Datenschutzrecht künftig konzeptionell modernisiert werden, um risikoadäquat auf allgegenwärtige Datenverarbeitung einzugehen und dabei auch das Recht auf informationelle Selbstbestimmung stärker zu schützen?

Bereits im Jahre 2001 hatte ROSSNAGEL im Auftrag des Bundesministeriums ein erstes Gutachten zur Modernisierung des Datenschutzrechts vorgestellt. In seinem neuesten, darauf aufbauenden Gutachten „Datenschutz in einem informatisierten Alltag“ (2007) stellt er zehn Grundsätze für eine mögliche Neuorientierung der bestehenden Gesetze dar, deren Grundgedanken im Folgenden zusammenfassend vorgestellt werden. Unter dem Grundsatz „*Informationelle Selbstbestimmung durch Opt-in*“ wird eine grundsätzlich notwendige Handlungspflicht des Verarbeiters beschrieben, wenn dieser personenbezogene Daten erheben möchte. Der Betroffene soll zunächst mit dem Ansinnen der verantwortlichen Stelle konfrontiert werden und kann darauf reagieren. Gegenwärtig ermöglicht die gesetzliche Generalklausel des „berechtigten Interesses“[133] in der Praxis nahezu jede gewünschte Datenverarbeitung. Das heutige „Opt-out“ erfordert die Initiative des Betroffenen, gegen diese Datenerhebung vorzugehen, soweit dies ihm möglich ist. Durch die Umkehr der Handlungspflicht zu Gunsten des Betroffen soll Datenschutz bereits vor der Erhebung stattfinden.

Der Grundsatz *„Gestaltungs- und Verarbeitungsregeln“* fordert, dass der Fokus des Datenschutzrechtes nicht – wie gegenwärtig der Fall – auf der Frage der Zulässigkeit einer Datenerhebung liegen soll, sondern auf permanent wirkenden Gestaltungs- und Verarbeitungsregeln. Technisch auswertbare Signalisierungen könnten dabei Datenerhebungen transparenter machen und eine Unterscheidung zwischen einer Datenverarbeitung mit und ohne gezielten Personenbezug könnte den Datenschutz zusätzlich

---

[131] TAUCIS (2006), S. 199

[132] ROSSNAGEL, A. (2007B), S. 126

[133] §28 Absatz 1 Satz 1 Nr. 2 und Absatz 3 Nr. 1 BDSG

vereinfachen.[134] So könnte auf eine vorherige Unterrichtung des Betroffenen verzichtet werden, wenn der Zweck der Datenerhebung nur der Erfüllung einer technischen Dienstleistung dient und kein Personenbezug beabsichtigt ist. In diesem Falle müsste die Verwendung der erhobenen Daten aber auch nur auf diesen Zweck begrenzt werden. Zur Unterstützung dieser Zweckbindung sollte ein Verstoß mit einem Bußgeld bestraft werden. Im Grundsatz *„Datenschutz durch Technik“* wird dargestellt, dass das Datenschutzrecht die Voraussetzungen für einen Datenschutz durch Technik schaffen muss, indem Pflichten und Anreize geschaffen werden sollen, um Datenschutztechniken einzusetzen. *„Was technisch verhindert wird, muss nicht verboten werden“,* so ROSSNAGEL. Im Rahmen von „*Vorsorgeregelungen*“ könnte Risiken der Profilbildung entgegengewirkt werden, wenn beispielsweise eine nachträgliche Herstellung eines Personenbezuges von nicht personenbezogenen Daten verboten würde und eine Übermittlung solcher Daten nur an Dritte zulässig wäre, wenn sichergestellt ist, dass diese keinen Personenbezug herstellen können. Unter dem Grundsatz *„Freiheitsfördernde Architekturen“* wird gefordert, dass bei der infrastrukturellen Ausgestaltung allgegenwärtiger Datenverarbeitung ihre Nützlichkeit von ihrem Kontrollpotenzial getrennt wird. Zudem sollen Räume und Zeiten berücksichtigt werden, in denen keine Datenerhebung stattfindet, und es muss rechtlich gewährleistet sein, dass es für allgegenwärtige Datenverarbeitung keinen „Anschluss- und Benutzungszwang“ gibt. Unter dem Grundsatz *„Neue Regelungsadressaten“* sollen diejenigen Adressaten zur Verantwortung gezogen werden, die auch entsprechende Handlungsmöglichkeiten haben. Diese sind nicht zwangsläufig die Betreiber der Datenverarbeitungssysteme oder die Betroffenen, sondern insbesondere die Entwickler solcher Systeme. Daten werden nicht nur durch den Staat oder durch Unternehmen erhoben. Eine Vielzahl an Daten wird auch von Privatpersonen erhoben und verursacht dadurch ein Risiko für die informationelle Selbstbestimmung anderer. Unter dem Grundsatz *„Einbezug privater Datenverarbeitung“* wird vorgeschlagen, dass künftig auch Einzelregelungen für die Datenerhebung aus dem persönlichen und familiären Bereich berücksichtigt werden sollen. Diese sind im jetzigen Datenschutzrecht vollkommen ausgenommen. Datenschutz wird sich nur dann ganzheitlich umsetzen lassen, wenn jeder auch in seiner Mitwirkung und Umsetzung einen Eigennutzen hat. Im Grundsatz *„Anreize und Belohnungen“* werden daher rechtliche Rahmenbedingungen vorgeschlagen, welche Zertifikate und freiwillige Datenschutzaudite ausloben, wenn Datenschutz in ausreichendem Maß gewahrt wird. Datenschutz soll damit als Werbeargument

---

[134] ROSSNAGEL, A. (2007B), S. 181

und Wettbewerbsvorteil angesehen werden. Im Grundsatz der *„Gefährdungshaftung“* fordert ROSSNAGEL die Einführung einer Gefährdungshaftung im privatwirtschaftlichen Bereich, um Schadensersatzregelungen für Betroffene zu erleichtern und dadurch eine präventive Wirkung zu erreichen. Diese Gefährdungshaftung besteht gegenwärtig nur für den öffentlichen Bereich.[135] Im nicht-öffentlichen Bereich gilt dagegen nur eine Verschuldungshaftung mit Beweislastumkehr, welche jedoch entfällt, wenn die verantwortliche Stelle die gebotene Sorgfalt beachtet hat. Im letzten Grundsatz, *„Institutionalisierte Grundrechtskontrolle“,* werden besser ausgestattete Kontrollstellen gefordert, welche nicht nur die individuellen Daten prüfen, sondern ganze Systeme mit ihren Funktionen und Strukturen.
Zusammenfassend beschreibt ROSSNAGEL die Notwendigkeit einer objektivierten Ordnung der Datenverarbeitung und -kommunikation bei professioneller Kontrolle, mit vorsorgender Gestaltung von Strukturen und Systemen, der Inpflichtnahme von Herstellern zur Umsetzung von Datenschutz in Technik sowie der Nutzung von Eigennutz durch Anreize zu datenschutzgerechtem Handeln.[136]

7 Zusammenfassung

Zielsetzung dieser Arbeit war die Entwicklung eines Anwendungsszenarios für das Internet der Dinge im Bereich der privaten Beobachtung. Die zentrale Fragestellung war dabei, wie stark der Einsatz der RFID-Technologie künftig zu Beobachtung, Verknüpfung und Auswertung von Konsumentenverhalten sowie der Ausnutzung von privaten Daten führen kann.
Um eine mögliche Antwort auf diese Fragestellung geben zu können, war es zunächst notwendig, einige thematische Grundlagen aufzubauen. Dabei hat sich herausgestellt, dass sich die RFID-Technologie rasant in immer mehr Anwendungsbereichen etabliert, jedoch noch nicht den Massenmarkt erreicht hat. Erst wenn dies erfolgen wird, könnte sich darauf aufbauend ein Internet der Dinge entwickeln. Das EPC-Netzwerk könnte dabei als technologische Infrastruktur dienen. Dem stehen jedoch zahlreiche Bedenken von Datenschützern und Verbraucherschutzorganisationen entgegen. Das zu schützende Gut stellen die informelle Privatheit und das Recht auf informationelle Selbstbestimmung dar, welche als unverzichtbare Voraussetzung einer freien Meinungsbildung und damit als wesentliche Grundsäule unserer demokratischen Gesellschaft angesehen werden. Es wurden

[135] §8 BDSG

[136] ROSSNAGEL, A. (2007B), S. 200

vier Grenzbereiche beschrieben, deren Überschreitung eine Verletzung der Privatsphäre von Individuen darstellen kann: natürliche Grenzen, soziale Grenzen, räumliche und zeitliche Grenzen sowie Grenzen flüchtiger Situationen. Es wurde dargestellt, dass die RFID-Technologie wesentliches Potenzial hat, alle Grenzbereiche zu überschreiten. Konkret wurden hier fünf Gefahrenbereiche für die Privatheit beschrieben, welche bei einer massenhaften Anwendung dieser Technologie entstehen könnten: das unbemerkte Auslesen durch Dritte, die Verfolgbarkeit von Personen durch ihre Objekte, das Auffinden sozialer Netzwerke, die Verantwortlichkeit für Objekte sowie die Bevormundung durch Technik. Schutzmaßnahmen in Form von freiwilligen Selbstverpflichtungen für Anwender oder technische Datenschutz-Technologien könnten die Sicherheit der Verbraucher erhöhen, haben sich bisher aber noch nicht durchsetzen können.

Im weiteren Verlauf der Arbeit wurde ein Anwendungsszenario für das Internet der Dinge entwickelt. Um dabei willkürliche Behauptungen zu vermeiden und um eine bessere Nachvollziehbarkeit zu gewährleisten, wurde die Szenario-Technik als wissenschaftliche Methode angewandt. Sie ermöglicht unter Berücksichtigung von quantitativen und qualitativen Informationen über die Einflussfaktoren die Entwicklung verschiedener, stets plausibler Zukunftsszenarien des Untersuchungsgegenstandes.

Im Rahmen der Szenario-Entwicklung wurden fünf Einflussfelder auf die zukünftige Entwicklung des Internets der Dinge identifiziert: Technik, Standardisierung, Wirtschaftlichkeit, Akzeptanz, Gesetzgebung und internationaler Wettbewerb. Im weiteren Verlauf der Arbeit wurden aus diesen Einflussfeldern einzelne Einflussfaktoren zu Deskriptoren zusammengefasst und sowohl in ihrem jetzigen als auch in zwei möglichen Zukunftsausprägungen modelliert. Im Ergebnis sind so zwei unterschiedliche Zukunftsszenarien entstanden, welche im Rahmen von Geschichten beispielhafte Anwendungen im Bereich der privaten Beobachtung illustrieren. Die Gefahren im Hinblick auf die private Beobachtung sind in beiden Szenarien unterschiedlich stark ausgeprägt. Es hat sich gezeigt, dass eine starke Verbreitung des Internets der Dinge nicht unbedingt zu einer stärkeren Gefahr im Hinblick auf die private Beobachtung führen muss. So führen im ersten Szenario stärkere Kontrollmöglichkeiten für Endnutzer und eine offene Informationspolitik von Arbeitgebern zu einer relativ sicheren Zukunft. Im zweiten Szenario ist das Internet der Dinge nur im gewerblichen Bereich etabliert, und trotzdem führt ein Datenskandal dazu, dass Verbraucherprofile unkontrollierbar in Umlauf geraten sind. Es sind natürlich noch unendlich viele weitere Szenarien denkbar. Anhand der dargestellten Szenarien konnten aber einige beispielhafte Anwendungen dargestellt werden, welche im Anschluss rechtlich bewertet

wurden. Eine rechtliche Bewertung der illustrierten Anwendungen war nur unter Berücksichtigung der jeweils beschriebenen Umfeldfaktoren möglich. Für die Anwendbarkeit von Gesetzen spielt dabei die Rolle des Betroffenen, dessen Umfeld und seine Handlungsmöglichkeiten eine entscheidende Rolle. Als relevante Gesetze wurden neben dem BDSG vor allem das Verbraucherschutzgesetz, das Arbeitsrecht sowie Betriebsvereinbarungen dargestellt.

Die durchgeführte rechtliche Bewertung hat zusammenfassend gezeigt, dass in einfach strukturierten Anwendungen – wenn also der Zweck der Datenerhebung und die Rollen der Beteiligten klar bestimmbar sind – das BDSG einen ausreichenden Schutz der Privatsphäre darstellen kann. Durch die 1995 verabschiedete Richtlinie 95/46/EG ist dieser Schutz nicht nur in Deutschland, sondern auch in anderen europäischen Ländern gewährleistet. Ob dieser Schutz jedoch auch praktisch umsetzbar ist, vor allem wenn in zukünftigen komplexen Anwendungen die Rollen der Betroffen ständig wechseln oder wenn die Datenverarbeitung spontan und unbemerkt für vielfältige Zwecke erfolgt, ist zweifelhaft.

Eine Lösung könnte hier in einer risikoadäquaten Modernisierung des BDSG liegen. Es wurde dargestellt, dass diese Modernisierung hauptsächlich konzeptionell erfolgen müsste, indem neue Grundsätze für den Umgang mit Daten definiert werden.

Zurückkommend auf die ursprüngliche Fragestellung dieser Arbeit, wie stark der Einsatz von RFID-Technologie zu einer Beobachtung im privaten Bereich führen kann, muss im Hinblick auf die dargestellten Ergebnisse dieser Arbeit die Anwort heißen: „Es kommt darauf an." Fest steht, dass nicht über Nacht allgegenwärtige Datenverarbeitung Einzug in unseren Alltag halten wird. Aber die RFID-Technologie, Handy-Kameras und Location Based Services stellen für ROSSNAGEL Vorboten einer großen, technikgetriebenen Umwälzung der Verhältnisse dar. Ihm zufolge wäre es fahrlässig, diese Entwicklungsperspektiven zu ignorieren, und es sei die Pflicht des Gesetzgebers, unsere Grundrechte und die demokratische Struktur unserer Gesellschaft zu schützen.[137] Noch bleibt genug Zeit, uns auf diese neuen Bedingungen einzurichten und Maßnahmen zum Schutze unserer informationellen Selbstbestimmung zu finden. Bei vielen technologischen Fortschritten waren die Bedenken zu Anfang stets groß, jedoch würde heute niemand mehr die Fotografie, den Druck, das Mobiltelefon oder auch das Internet vermissen wollen.

---

[137] BVerfGE 49, 89, (140)

Anhang

Dieser Arbeit liegt eine CD-ROM bei.

Inhalt der CD-ROM:

- Sämtliche Internetquellen als HTML-Archiv
- Alle verwendeten Berichte und Studien, sofern diese als PDF-Datei verfügbar waren.
- Die Arbeitsdaten dieser Arbeit im DOC und DOCX-Format
- Das Exposé der Anmeldung
- Die Diplomarbeit samt Titelblatt als PDF-Datei

Literaturverzeichnis

ALBERS, O., BROUX, A. (1999): *Zukunftswerkstatt und Szenariotechnik.*
Weinheim und Basel, Beltz, 1999

ALBRECHT, K., MCINTYRE, L. (2006): *Spychips. How major corporations and government plan to track your every purchase and watch your every move.*
Penguin Group, New York, 2006

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

BERTELSMANN-STIFTUNG.DE (2006): *USA verlieren international ihr Monopol als Großmacht – nur Minderheit der Deutschen sieht die Bundesrepublik noch als Global Player***.**
http://www.bertelsmann-stiftung.de/cps/rde/xchg/SID-0A000F0A82A71546/bst/hs.xsl/nachrichten_29056.htm am 22.04.2009

BERTHOLD, O., GÜNTHER, O., SPIEKERMANN, S. (2005): *RFID – Verbraucherängste und Vebraucherschutz*. Wirtschaftsinformatik 47, Nr. 6, S. 422-430, 2005

BMI (2008): *Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie*.
Drucksache 16/7891, Berlin, 2008

BMWI (2007A): *RFID: Potenziale für Deutschland*.
Bundesministerium für Wirtschaft und Technologie (BMWi), Berlin 2007

BMWI (2007B): *European Policy Outlook RFID*.
Bundesministerium für Wirtschaft und Technologie (BMWi), Berlin 2007

BOHN, J., COROAMA, V., LANGHEINRICH, M., MATTERN, F., ROHS, M. (2003): *Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge.* In: Ralf Grötker (Ed.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Heise-Verlag, S. 195-245, 2003

BORCHERT, G. (1994): *Verbraucherschutzrecht*. München, 1994

BREHM, S., BREHM, J. (1981): *Psychological Reactance: A Theory of Freedom and Control*. San Diego, 1981

BSI (2004): *Risiken und Chancen des Einsatzes von RFID-Systemen*, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2004

DAVIS (1989): *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly 13(3), S. 319-340, 1989

DUDEN WIRTSCHAFT (2004): *Grundlagenwissen für Schule und Studium, Beruf und Alltag.* 2. Auflage, Mannheim: Bibliographisches Institut & F.A. Brockhaus 2004. Lizenzausgabe Bonn: Bundeszentrale für politische Bildung, 2004

EC (2008): *Communication on future networks and the internet.* Commission staff working document, SEC(2008) 2507, SEC(2008) 2516, Commission of the European Communities, Brussels, 2008

EPCGLOBAL (2006): *EPCglobal Tag Data Standards Version 1.3.* http://www.epcglobalinc.org/standards/tds/tds_1_3-standard-20060308.pdf

EPIS-REPORT (2008): *Report on the Creative Content Industry*. Friedewald, M.; Weber,M.; Juan, M. et al., European Perspectives on the Information Society (EPIS), 2008

FAZIT-FORSCHUNG (2008): *Die IT- und Medienwelt in Baden-Württemberg im Jahre 2020.* Beckert, B., Goluchowicz, K., Kimpeler, S., Forschungsbericht Band 15, MFG Stiftung Baden-Württemberg, Stuttgart, 2008

FERSCHA, A. (2007): *Pervasive Computing: connected > aware >smart.* In: Friedemann Mattern (Ed.): Die Informatisierung des Alltags – Leben in smarten Umgebungen. Springer, S. 3-10, Berlin, Heidelberg, New York, 2007

FINK, A., Schlake, O., Siebe, A. (2002): *Erfolg durch Szenario-Management*. 2. Auflage, Frankfurt, Campus, 2002

FINKENZELLER, K. (2002): *RFID-Handbuch*. 3. Auflage, Carl Hanser Verlag, München, Wien, 2002

FISHKIN, K., ROY, S. (2003): *Enhancing RFID Privacy via Antenna Energy Analysis.* RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

FLEISCH, E., MATTERN, F., BILLINGER, S. (2004): *Betriebswirtschaftliche Auswirkungen des Ubiquitous Computing, Beispiele, Bausteine und Nutzenpotentiale*. Heinz Sauerburger (Ed.): Ubiquitous Computing. HMD 229 – Praxis der Wirtschaftsinformatik, dpunkt.verlag, S. 5-15, 2003

FLUSSMANN, N. (2001): *Lexikon der Kommunikations- und Informationstechnik*. 3.Auflage, Heidelberg, 2001

FRIEDEWALD, M. (2007): *Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenarioanalyse.* In: Friedemann Mattern (Ed.): Die Informatisierung des Alltags – Leben in smarten Umgebungen. Springer, S. 207-231, Berlin, Heidelberg, New York, 2007

GARFINKEL, S., JUELS, A., PAPPU R. (2005): *RFID privacy: an overview of problems and proposed solutions (Computer Society).* IEE Security and Privacy, auf www.simson.net/clips/academic/2005.IEEE.RFID.pdf

GS1 (2005): *Internet der Dinge. Management Information.* GS1 Germany GmbH, Köln, 2005

HASENKAMP, U. (2008): *Wirtschaftliche Aspekte der allgegenwärtigen Datenverarbeitung.* In: Alexander Rossnagel, Tom Sommerlatte, Udo Winand (Eds.): Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien. Springer, S. 109-112, Berlin, Heidelberg, New York, April 2008

INFORMATIONSFORUM RFID (2008): *Rechtliche Dimensionen der Radiofrequenz-Identifikation.* Informationsforum RFID e.V., Berlin, 2008

INFORMATIONWEEK.COM (2008): *Washington State Gov. Signs RFID Privacy Protection Law.* http://www.informationweek.com/news/mobility/showArticle.jhtml?articleID=207000102 am 22.04.2009

JUELS, A., RIVEST, R., SZYDLO, M. (2003): *The Blocker Tag: Selective Blocking of RFID-Tags for Consumer Privacy.* www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker

KNEBEL, U.; LEIMEISTER, J. M.; KRCMAR, H. (2007): *Wahrgenommene strategische Bedeutung von RFID aus Sicht von IT-Entscheidern in Deutschland – Eine empirische Analyse.* In: Wirtschaftsinformatik 2007 (Vol. 1), Universitätsverlag Karlsruhe, S. 89-106, Karlsruhe 2007

LANDT, J. (2001): *Shrouds of Time. The History of RFID*. **WWW.RFIDCONSULTATION.EU** http://www.rfidconsultation.eu/docs/ficheiros/shrouds_of_time.pdf 4.4.2008

LANGHEINRICH, M. (2004): *Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie.* In: Elgar Fleisch, Friedemann Mattern (Eds.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Springer, S. 329-362, Berlin Heidelberg New York, 2005

LANGHEINRICH, M. (2007): *Gibt es in einer total informatisierten Welt noch eine Privatsphäre?*
In: Friedemann Mattern (Ed.): Die Informatisierung des Alltags – Leben in smarten Umgebungen. Springer, S. 233-264, Berlin Heidelberg New York, 2007

LANGHEINRICH, M. (2008): *RFID und die Zukunft der Privatsphäre.*
In: Alexander Rossnagel, Tom Sommerlatte, Udo Winand (Eds.): Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien. Springer, S. 43-68, Berlin, Heidelberg, New York, 2008

LANTERMANN, E. (2008): *Gesellschaftliche Antworten auf allgegenwärtige Datenverarbeitung.*
In: Alexander Rossnagel, Tom Sommerlatte, Udo Winand (Eds.): Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien. Springer, S. 185-194, Berlin, Heidelberg, New York, 2008

MAREK, C. (2007): *RFID – Kosten und Nutzen: Eine wirtschaftliche Analyse.* VDM Verlag Dr. Müller; 1. Auflage, Saarbrücken, 2007

MATTERN, F. (2003): *Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing.* In: Friedemann Mattern (Ed.): Total vernetzt. Springer, S. 1-41, Berlin, Heidelberg, New York, April 2003

MATTERN, F. (2005): *Die technische Basis für das Internet der Dinge.* In: Elgar Fleisch, Friedemann Mattern (Eds.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Springer, S. 39-66, Berlin, Heidelberg, New York, 2005

MATTERN, F. (2007): *Acht Thesen zur Informatisierung des Alltags.* In: Friedemann Mattern (Ed.): Die Informatisierung des Alltags – Leben in smarten Umgebungen. Springer, S. 11-16, Berlin, Heidelberg, New York, 2007

MATTERN, F. (2008): *Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen.* In: Alexander Rossnagel, Tom Sommerlatte, Udo Winand (Eds.): Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien. Springer, S. 3-29, Berlin, Heidelberg, New York, April 2008

MEADOWS, D.L., MEADOWS, D.H. ZAHN, E. (1972): *Die Grenzen des Wachstums. Bericht des Club of Rome zur Lage der Menschheit.* Stuttgart, Deutsche Verlags-Anstalt, 1972

NOKIA.DE (2009): *Bedienungsanleitung des Nokia 5140 Mobiltelefon.* http://www.nokia.de/service-und-software/produktservice/nokia-5140/bedienungsanleitung am 7.4.2009

PESLAK, A. (2005): *An Ethical Exploration of Privacy and Radio Frequency Identification*, Journal of Business Ethics (2005) Springer, S. 327–345, Berlin, Heidelberg, New York, 2005

PRODUKTION (2008): *RFID soll vor Billig-Imitaten schützen.* Produktion. Die Wirtschaftszeitung für die deutsche Industrie. Ausgabe 42/2008, Verlag moderne Industrie, Landsberg, 2008

RFID-READY.DE (2009): *Standardisierung von RFID.*
http://www.rfid-ready.de/standardisierung-von-rfid.html am 22.04.2009

RFID-BASIS (2007): *Laser-Technik als Alternative zu RFID.*
http://www.rfid-basis.de/article-0054.html am 22.04.2009

RÖSSLER, BEATE (2001): *Der Wert des Privaten*, Frankfurt am Main, 2001

ROSSNAGEL, A. (2007): *Informelle Selbstbestimmung in der Welt des Ubiquitous Computing.* In: Friedemann Mattern (Ed.): Die Informatisierung des Alltags – Leben in smarten Umgebungen. Springer, pp. 265-289, Berlin Heidelberg New York, 2007

ROSSNAGEL, A. (2007B): *Datenschutz in einem informatisierten Alltag.* Stabsabteilung der Friedrich-Ebert-Stiftung, Berlin, 2007

SARMA, S., WEIS S., ENGELS, D. (2002): *RFID Systems and Security and Privacy Implications.* Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Redwood Shores, USA, Springer, Berlin, Heidelberg, New York, 2002

SCHAAR, P. (2007): *Das Ende der Privatsphäre*. München, Bertelsmann Verlag, 2007

SPIEGEL.DE (2008): *Telekom bespitzelte auch eigene Mitarbeiter*.
http://www.spiegel.de/wirtschaft/0,1518,586516,00.html am 22.04.2009

SPIEKERMANN, S., ROTHENSEE, M.: (2005): *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing.*
Institut fur Wirtschaftsinformatik Humboldt-Universität zu Berlin

SPIEKERMANN, S., ZIEKOW, H. (2006): *RFID: a Systematic Analysis of Privacy Threats & a 7-point plan to address them*.
Journal of Information Systems Security, Vol. 1, Nr. 3, 2006

STRASSNER, M., FLEISCH, E., (2005): *Innovationspotenzial von RFID für das Supply-Chain-Management*. Wirtschaftsinformatik 47, Nr 1, 2005, S.45-54

TAGESSCHAU.DE (2009): *Winzige Helfer mit Schnüffelpotenzial.*
http://www.tagesschau.de/inland/meldung45694.html am 7.4.2009

TAUCIS (2006): *Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung*. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Humbold Universität zu Berlin (HU), Berlin, 2006

TINNEFELD, M. (2007): Neue Juristische Wochenschrift (2007), S. 626

VDEB (2006): *Management-Leitfaden für den Einsatz von RFID-Systemen.* RFID-Fachgruppe, Verband der EDV-Software- und -Beratungsunternehmen e.V. (VDEB) in Zusammenarbeit mit dem Industrieverband für Automatische Identifikation, Datenerfassung und Mobile Datenkommunikation (AIM Deutschland), Aachen, 2006

WIKIPEDIA.DE (2009): *Radio Frequency Identification.* http://de.wikipedia.org/wiki/Radio_Frequency_Identification am 26.04.2009

Eidesstattliche Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten und nicht veröffentlichten Schriften entnommen sind, sind als solche kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form noch nicht als Prüfungsarbeit eingereicht worden.

Aachen, 28.05.2009

Patrick Heinker